

Prestige 782R

G.SHDSL Router

User's Guide

Version 2.50

February 2001

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Copyright

Copyright © 2001 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2. 1077(a)



The following equipment:

Product Name : SDSL/G.SHDSL Router/Bridge
 Trade Name : ZyXEL Communications Corporation
 Model Number : PRESTIGE 742R, PRESTIGE 742M, PRESTIGE 782R,
 PRESTIGE 782M

It's herewith confirmed to comply with the requirements of FCC Part 15 Rules.

Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

The result of electromagnetic emission has been evaluated by QuieTek EMC laboratory (NVLAP Lab. Code : 200347-0) and showed in the test report.
 (Report No. : QTK-009H068F)

It is understood that each unit marketed is identical to the device as tested, and Any changes to the device that could adversely affect the emission Characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:

Company Name ZYXEL communications, corp.
 Company Address 1650 Miraloma Avenue
 Telephone (714)632-0882 Facsimile : (714)632-0858

Person is responsible for marking this declaration:

Gordon Yang
 Name (Full name)

President
 Position / Title

10/20/00
 Date


 Legal Signature

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Notice 2

Shielded RS-232C cables are required to be used to ensure compliance with FCC Part 15, and it is the responsibility of the user to provide and use shielded RS-232C cables.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operation and safety requirements. The Industry Canada label does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.



Declaration of Conformity

The following products is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility Directive (89/336/EEC). The listed standard as below were applied:

The following Equipment:

Product : SDSL/G.SHDSL Router/Bridge
Model Number : PRESTIGE 742R, PRESTIGE 742M, PRESTIGE 782R,
PRESTIGE 782M

RFI Emission: Generic emission standard according to EN 50081-1:1992
Limit class B according to EN 55022/1998
Limits class A for harmonic current emission according to EN 61000-3-2:1995
Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity : Generic immunity standard according to EN 50082-1:1997/ EN 55024: 1998
Electrostatic Discharge according to EN 61000-4-2:1995
Contact Discharge: 4 kV, Air Discharge : 8 kV
Radio-frequency electromagnetic field according to EN 61000-4-3:1996
80 - 1000MHz with 1kHz AM 80% Modulation: 3V/m
Electrical fast transient/burst according to EN 61000-4-4:1995
AC/DC power supply: 1kV, Data/Signal lines : 0.5kV
Surge immunity test according to EN 61000-4-5:1995
AC/DC Line to Line: 1kV, AC/DC Line to Earth : 2kV
Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996
0.15 - 80MHz with 1kHz AM 80% Modulation: 3V/m
Power frequency magnetic field immunity test according to EN 61000-4-8:1993
3A/m at frequency 50Hz
Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994
30% Reduction @ 10ms >95% Reduction @500ms, >95%Reduction @10ms/ 5000ms

The following importer/manufacture is responsible for this declaration:

Company Name **ZyXEL** Communications Services GmbH.
Company Address :Thaliastrasse 125a/2/2/4
A-1160 Wien • AUSTRIA
Telephones : Tel.: 01 / 494 86 77-0 Facsimile :
Fax: 01 / 494 86 78

Person is responsible for marking this declaration:

Manfred RECLA
Name (Full Name)
October 17, 2000
Date

ZyXEL European Techn. Support
Position/ Title
Manfred Recla
Legal Signature
ZyXEL Communications Services GmbH.



Declaration of Conformity

We, the Manufacturer/Importer

ZyXEL Communications Services GmbH.

Thaliastrasse 125a/2/2/4

A-1160 Vienna – AUSTRIA

declare that the product

Prestige 782R

is in conformity with

(Reference to the specification under which conformity is declared)

Standard	Standard Item	Version
EN 55022	Radio disturbance characteristics – Limits and method of measurement.	1994
EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
EN 61000-4-2	Electrostatic discharge immunity test – Basic EMC Publication.	1995
EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test.	1996
EN 61000-4-4	Electrical fast transient/burst immunity test – Basic EMC Publication.	1995
EN 61000-4-5	Surge immunity test.	1995
EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields.	1996
EN 61000-4-8	Power Magnetic Measurement.	1993
EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests.	1994

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.



Online Registration

Do not forget to register your Prestige (fast, easy online registration at www.zyxel.com) for free future product updates and information.

Customer Support

Please have the following information ready when you contact customer support:

- Prestige Model and serial number.
- Information in **Menu 24.2.1 –System Information**.
- Warranty Information.
- Date that you received your Prestige.
- Brief description of the problem and the steps you took to solve it.

METHOD	EMAIL – SUPPORT	TELEPHONE	WEB SITE	REGULAR MAIL
REGION	EMAIL – SALES	FAX	FTP SITE	
WORLDWIDE	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	support@europe.zyxel.com		www.europe.zyxel.com	
	sales@zyxel.com.tw	+886-3-578-2439	ftp.europe.zyxel.com	
NORTH AMERICA	support@zyxel.com	+1-714-632-0882 800-255-4101	www.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.zyxel.com	
SCANDINAVIA	support@zyxel.dk	+45-3955-0700	www.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	sales@zyxel.dk	+45-3955-0707	ftp.zyxel.dk	
AUSTRIA	support@zyxel.at	+43-1-4948677-0 0810-1-ZyXEL 0810-1-99935	www.zyxel.at	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria
	sales@zyxel.at	+43-1-4948678	ftp.zyxel.at Note: Austrian users with *.at domain only!	
GERMANY	support@zyxel.de	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935 RMA/Repair hotline	www.zyxel.de	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuersele, Germany.
	sales@zyxel.de	+49-2405-6909-99	ftp.europe.zyxel.com	

Table of Contents

Copyright	ii
Warranty	viii
Customer Support	ix
List of Figures	xiv
List of Tables	xvii
Preface	xix
What is xDSL?	xxi
PART I GETTING STARTED.....	I
Chapter 1 Getting to Know Your G.SHDSL Router	1-1
1.1 Features of the Prestige	1-1
1.2 Application Scenarios for the Prestige	1-4
1.2.1 Internet Access	1-4
1.2.2 LAN-to-LAN Application	1-4
Chapter 2 Hardware Installation and Initial Setup	2-1
2.1 Installation Requirements	2-1
2.2 Front Panel LEDs of the Prestige 782R	2-1
2.3 Rear Panel and Connections of the Prestige 782R	2-2
2.4 Turning On Your Prestige	2-3
2.5 Navigating the SMT Interface	2-4
2.6 SMT Menu Commands	2-5
2.6.1 System Management Terminal Interface Summary	2-7
2.7 Changing the System Password	2-7
2.8 Resetting the Prestige	2-8
2.9 General Setup	2-9
2.9.1 Note on Bridging	2-10
2.10 Setting Up the WAN Link	2-10
2.10.1 Service Type	2-10
2.10.2 Rate Adaption	2-10
2.10.3 Transfer Rates	2-10
2.10.4 Standard Mode	2-11
2.11 Ethernet Setup	2-11
2.11.1 LAN Setup	2-12
2.11.2 Protocol Dependent Ethernet Setup	2-12
Chapter 3 Internet Access	3-1
3.1 Ethernet Factory Defaults	3-1
3.2 TCP/IP and DHCP Ethernet Setup: DHCP	3-1
3.2.1 DHCP Setup	3-1
3.2.2 Client IP Pool Setup	3-1
3.2.3 DNS Server Address	3-2

3.2.4	TCP/IP and DHCP Ethernet Setup: TCP/IP	3-2
3.2.5	IP Address and Subnet Mask	3-2
3.2.6	RIP Setup	3-3
3.2.7	Multicast	3-4
3.2.8	IP Policies	3-4
3.2.9	Configuring TCP/IP and DHCP Ethernet Setup	3-5
3.2.10	IP Alias.....	3-7
3.2.11	IP Alias Setup.....	3-7
3.3	LANs and WANs.....	3-9
3.3.1	LANs, WANs and the Prestige	3-9
3.4	Internet Access Configuration.....	3-9
3.4.1	VPI and VCI	3-10
3.4.2	Multiplexing.....	3-10
3.4.3	Encapsulation.....	3-10
3.4.4	IP Address Assignment.....	3-11
3.4.5	Internet Account Information.....	3-11
3.4.6	Traffic Shaping	3-12
3.5	Internet Access Configuration.....	3-13
3.6	Single User Account.....	3-15
3.6.1	Advantages of SUA.....	3-16
3.6.2	Single User Account Configuration	3-16
3.7	Multiple Servers Behind the SUA.....	3-17
3.7.1	Configuring a Server Behind the SUA	3-17
PART II ADVANCED APPLICATIONS		II
Chapter 4 Remote Node Configuration		4-1
4.1	Remote Node Setup.....	4-1
4.1.1	Remote Node Profile.....	4-1
4.1.2	Encapsulation and Multiplexing Scenarios	4-2
4.1.3	Outgoing Authentication Protocol	4-4
4.1.4	Editing PPP Options.....	4-4
4.2	Remote Node Setup.....	4-5
4.3	Remote Node Filter	4-8
Chapter 5 Remote Node TCP/IP Configuration		5-1
5.1	TCP/IP Configuration	5-1
5.1.1	Editing TCP/IP Options	5-1
5.1.2	IP Static Route Setup	5-5
Chapter 6 IPX Configuration.....		6-1
6.1	IPX Network Environment.....	6-1
6.1.1	Network and Node Number	6-1
6.1.2	Frame Types.....	6-1
6.1.3	External Network Number	6-2
6.1.4	Internal Network Number	6-2

6.2	The Prestige in an IPX Environment.....	6-3
6.2.1	The Prestige on a LAN with a Server	6-3
6.2.2	The Prestige on a LAN without Server	6-3
6.3	IPX Ethernet Setup	6-4
6.4	LAN-to-LAN Application With Novell IPX.....	6-4
6.4.1	IPX Remote Node Setup.....	6-5
6.4.2	IPX Static Route Setup	6-6
Chapter 7	Bridging Setup.....	7-1
7.1	Bridging in General.....	7-1
7.2	Bridge Ethernet Setup	7-1
7.2.1	Remote Node Bridging Setup	7-2
7.2.2	Bridge Static Route Setup.....	7-3
PART III ADVANCED MANAGEMENT		III
Chapter 8	Filter Configuration	8-1
8.1	About Filtering	8-1
8.2	Configuring a Filter Set.....	8-3
8.2.1	Filter Rules Summary Menus	8-5
8.3	Configuring a Filter Rule	8-6
8.3.1	TCP/IP Filter Rule	8-6
8.3.2	Generic Filter Rule.....	8-10
8.3.3	Novell IPX Filter Rule	8-12
8.4	Filter Types and SUA.....	8-14
8.5	Filter Configuration Example	8-15
8.6	Applying Filters and Factory Defaults	8-18
8.6.1	Ethernet Traffic.....	8-18
8.6.2	Remote Node Filters	8-18
Chapter 9	SNMP Configuration.....	9-1
9.1	About SNMP.....	9-1
9.2	Supported MIBs.....	9-2
9.3	SNMP Configuration	9-2
9.4	SNMP Traps.....	9-4
Chapter 10	System Maintenance.....	10-1
10.1	System Status.....	10-1
10.1.1	System Information.....	10-4
10.1.2	Console Port Speed.....	10-4
10.2	Log and Trace	10-5
10.2.1	Viewing Error Log.....	10-5
10.2.2	Syslog and Accounting	10-5
10.3	Diagnostic	10-8
10.4	Filename Conventions.....	10-9
10.5	Backup Configuration.....	10-9
10.6	Restore Configuration.....	10-11

10.7	Upload Firmware.....	10-12
10.7.1	Upload Router Firmware.....	10-12
10.7.2	Uploading Router Configuration File.....	10-13
10.7.3	TFTP Transfer.....	10-14
	Using the FTP Command from the DOS Prompt.....	10-15
10.7.4	Boot Module Commands.....	10-17
10.8	Command Interpreter Mode.....	10-18
10.9	Time and Date Setting.....	10-18
Chapter 11	11-1
IP Routing Policy	11-1
11.1	Introduction.....	11-1
11.2	Benefits.....	11-1
11.3	Routing Policy.....	11-1
11.4	IP Routing Policy Setup.....	11-2
11.5	Applying an IP Policy.....	11-5
11.5.1	Ethernet IP Policies.....	11-5
11.6	IP Policy Routing Example.....	11-7
PART IV	ADDITIONAL INFORMATION.....	IV
Chapter 12	Troubleshooting.....	12-1
Appendix A	Power Adapter Specifications.....	A
Glossary	B
Index	M

List of Figures

Figure 1-1 Internet Access Application	1-4
Figure 1-2 LAN-to-LAN Application	1-5
Figure 2-1 Front Panel of Prestige 782R.....	2-1
Figure 2-2 Rear Panel of the Prestige 782R.....	2-2
Figure 2-3 Power-On Display	2-3
Figure 2-4 Login Screen.....	2-4
Figure 2-5 Prestige 782R SMT Menu Overview	2-5
Figure 2-6 SMT Main Menu	2-6
Figure 2-7 Menu 23 – System Password.....	2-7
Figure 2-8 Booting Up the Prestige.....	2-8
Figure 2-9 Menu 1 – General Setup.....	2-9
Figure 2-10 Menu 2 – WAN Setup.....	2-11
Figure 2-11 Menu 3 – Ethernet Setup	2-12
Figure 2-12 Menu 3.1 – LAN Port Filter Setup	2-12
Figure 3-1 Menu 3.2 – TCP/IP and DHCP Ethernet Setup	3-5
Figure 3-2 Physical Network.....	3-7
Figure 3-3 Partitioned Logical Networks.....	3-7
Figure 3-4 Menu 3.2.1 – IP Alias Setup.....	3-8
Figure 3-5 LAN and WAN IPs.....	3-9
Figure 3-6 Traffic Shaping.....	3-13
Figure 3-7 Menu 4 – Internet Access Setup.....	3-13
Figure 3-9 Single User Account Topology.....	3-15
Figure 3-10 Menu 4 – Internet Access Setup for Single User Account	3-16
Figure 3-11 SUA Server Configuration	3-18
Figure 4-1 Menu 11 – Remote Node Setup.....	4-1
Figure 4-2 Menu 11.1 – Remote Node Profile	4-2
Figure 4-3 Menu 11.2 – Remote Node PPP Options.....	4-5
Figure 4-4 Remote Node Network Layer Options	4-6
Figure 4-5 Menu 11.5 – Remote Node Filter	4-8
Figure 5-1 Menu 11.6 for VC-based Multiplexing.....	5-1
Figure 5-2 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation	5-2
Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection	5-3
Figure 5-4 Menu 11.3 – Remote Node Novell IPX Options	5-4
Figure 5-5 Sample Static Routing Topology.....	5-6
Figure 5-6 Menu 12 – Static Route Setup	5-6
Figure 5-7 Menu 12.1 – IP Static Route Setup.....	5-6
Figure 5-8 Edit IP Static Route	5-7
Figure 6-1 NetWare Network Numbers	6-2
Figure 6-2 Prestige in an IPX Environment	6-3

Figure 6-3 Menu 3.3 – Novell IPX Ethernet Setup	6-4
Figure 6-4 LAN-to-LAN Application With Novell IPX	6-5
Figure 6-5 Menu 11.3 – Remote Node Novell IPX Options	6-6
Figure 6-6 Menu 12.2.1 – Edit IPX Static Route	6-7
Figure 7-1 Menu 3.4 – Bridge Ethernet Setup.....	7-1
Figure 7-2 Menu 11.3 – Remote Node Bridging Options	7-2
Figure 7-3 Menu 12.3.1 – Edit Bridge Static Route	7-3
Figure 8-1 Outgoing Packet Filtering Process.....	8-1
Figure 8-2 Filter Rule Process.....	8-2
Figure 8-3 Menu 21 – Filter Set Configuration.....	8-3
Figure 8-4 Menu 21.1 – Filter Rules Summary.....	8-4
Figure 8-5 Menu 21.2 – Filter Rules Summary.....	8-4
Figure 8-6 Menu 21.1.1 – TCP/IP Filter Rule.....	8-7
Figure 8-7 Executing an IP Filter.....	8-9
Figure 8-8 Menu 21.1.1 – Generic Filter Rule	8-10
Figure 8-9 Menu 21.1.1 – IPX Filter Rule	8-12
Figure 8-10 Protocol and Device Filter Sets	8-15
Figure 8-11 Sample Telnet Filter.....	8-15
Figure 8-12 Sample Filter – Menu 21.3.1	8-16
Figure 8-13 Sample Filter Rules Summary – Menu 21.3.....	8-17
Figure 8-14 Filtering Ethernet Traffic	8-18
Figure 8-15 Filtering Remote Node Traffic.....	8-19
Figure 9-1 SNMP Management Model.....	9-1
Figure 9-2 Menu 22 - SNMP Configuration	9-3
Figure 10-1 Menu 24 – System Maintenance.....	10-1
Figure 10-2 Menu 24.1 – System Maintenance – Status	10-2
Figure 10-3 LAN Packet That Triggered Last Call.....	10-3
Figure 10-4 System Maintenance – Information.....	10-4
Figure 10-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed	10-5
Figure 10-6 Sample Error and Information Messages.....	10-5
Figure 10-7 Menu 24.3.2 – System Maintenance – Syslog and Accounting.....	10-6
Figure 10-8 Menu 24.4 – System Maintenance – Diagnostic.....	10-8
Figure 10-9 Backup Configuration.....	10-10
Figure 10-10 HyperTerminal Screen	10-10
Figure 10-11 Successful Backup	10-10
Figure 10-12 Restore Configuration.....	10-11
Figure 10-13 HyperTerminal Screen	10-11
Figure 10-14 Successful Restoration.....	10-12
Figure 10-15 Menu 24.7 – System Maintenance – Upload Firmware.....	10-12
Figure 10-16 Menu 24.7.1 – Uploading Router Firmware	10-13
Figure 10-17 Menu 24.7.2 – System Maintenance – Upload Router Configuration File.....	10-14
Figure 10-18 Sample FTP Session	10-16

Figure 10-19 Option to Enter Debug Mode	10-17
Figure 10-20 Boot Module Commands.....	10-18
Figure 10-21 Command Mode	10-18
Figure 10-22 System Maintenance – Time and Date Setting	10-19
Figure 11-1 IP Routing Policy Setup	11-2
Figure 11-2 Menu 25.1 – Sample IP Routing Policy Setup	11-3
Figure 11-3 IP Routing Policy.....	11-4
Figure 11-4 Menu 3.2 – TCP/IP and DHCP Ethernet Setup	11-6
Figure 11-5 Menu 11.3 – Remote Node Network Layer Options	11-6
Figure 11-6 Example of IP Policy Routing	11-7
Figure 11-7 IP Routing Policy Example	11-8
Figure 11-8 IP Policy Routing.....	11-9
Figure 11-9 Applying IP Policies.....	11-9

List of Tables

Table 2-1 LED Functions	2-1
Table 2-2 Main Menu Commands	2-6
Table 2-3 Main Menu Summary	2-7
Table 2-4 General Setup Menu Fields	2-9
Table 2-5 Menu 2 – WAN Setup	2-11
Table 3-1 DHCP Ethernet Setup Menu Fields.....	3-5
Table 3-2 TCP/IP Ethernet Setup Menu Fields	3-6
Table 3-3 IP Alias Setup Menu Fields	3-8
Table 3-4 Internet Account Information.....	3-12
Table 3-5 Internet Access Setup Menu Fields	3-14
Table 3-6 Single User Account Menu Fields.....	3-16
Table 3-7 Services and Corresponding Port Numbers.....	3-18
Table 4-1 Remote Node Profile Menu Fields.....	4-3
Table 4-2 Remote Node PPP Options Menu Fields.....	4-5
Table 4-3 TCP/IP-related Fields in Menu 11.1 – Remote Node Profile	4-6
Table 4-4 Remote Node TCP/IP Configuration.....	4-7
Table 5-1 TCP/IP-related Fields in Remote Node Profile	5-3
Table 5-2 TCP/IP Remote Node Configuration.....	5-4
Table 5-3 Edit IP Static Route Menu Fields	5-7
Table 6-1 Novell IPX Ethernet Setup Fields	6-4
Table 6-2 Remote Node Novell IPX Options	6-6
Table 6-3 Edit IPX Static Route Menu Fields	6-7
Table 7-1 Bridge Ethernet Setup Menu – Handle IPX Field Configuration	7-2
Table 7-2 Remote Node Bridge Options	7-3
Table 7-3 Edit Bridge Static Route Menu Fields.....	7-4
Table 8-1 Abbreviations Used in the Filter Rules Summary Menu.....	8-5
Table 8-2 Rule Abbreviations Used.....	8-5
Table 8-3 TCP/IP Filter Rule Menu Fields.....	8-7
Table 8-4 Generic Filter Rule Menu Fields	8-11
Table 8-5 IPX Filter Rule Menu Fields	8-13
Table 9-1 SNMP Configuration Menu Fields.....	9-3
Table 9-2 SNMP Traps.....	9-4
Table 9-3 Ports and Permanent Virtual Circuits	9-4
Table 10-1 System Maintenance – Status Menu Fields.....	10-2
Table 10-2 Fields in System Maintenance.....	10-4
Table 10-3 System Maintenance Menu – Syslog Parameters.....	10-6
Table 10-4 System Maintenance Menu – Diagnostic	10-8
Table 10-5 Filename Conventions.....	10-9
Table 10-6 Third Party FTP Clients – General Fields	10-16

Table 10-7 Time and Date Setting Fields	10-19
Table 11-1 IP Routing Policy Setup	11-3
Table 11-2 IP Routing Policy	11-4
Table 12-1 Problems Starting the Prestige	A
Table 12-2 Problems connecting with the WAN or Remote Node/ISP	A
Table 12-3 Problems connecting with the LAN	A

Preface

About Your Prestige

Congratulations on your purchase of the Prestige 782R G.SHDSL Router.

The Prestige is a high-performance router for Internet/LAN access via a telephone line. Your Prestige supports multi-protocol routing for TCP/IP and Novell IPX, as well as transparent bridging for other protocols.

The Prestige supports symmetrical multi-rate data transmission speeds from 144Kbps up to 2320Kbps. The actual rate depends on the copper category of your telephone wires, distance from the central office and the type of xDSL service you subscribe to. Its 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. See the following section for more background information on xDSL.

The Prestige uses TC-PAM line code with echo cancellation for high data rate transmissions over a single-twisted telephone wire pair without being affected by bridge taps or mixed cable links. It also provides high immunity from background noise.

Your Prestige is easy to install. You do not need to set any switches to configure it. Manage the Prestige via the SMT (System Management Terminal), a menu-driven interface, that you can access from either a terminal emulator or telnet. Or, use the CI commands that allow users to diagnose and test the Prestige using a specified set of commands.

Please visit our web site at www.zyxel.com for the latest release notes and product information.

About This User's Guide

This user's guide covers all operations of the Prestige. It will guide you through the correct configuration of your Prestige for various applications and show you how to get the best out of the many advanced features of your router.

Related Documentation

Related documentation includes:

- A Packing List Card that lists all items that come with your Prestige.
- A Read Me First document that will help get your Prestige up and running right away. It contains detailed easy-to-follow instructions, Prestige default settings, handy checklists and information on setting up your computer.
- A Support CD. This CD includes:
 - This User's Guide.
 - Support Notes (FAQ, Application Notes, Support Tools and CI Commands).
 - Links to the ZyXEL Website and Global Support Network.

Syntax Conventions

- “Type” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. Menu item choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity's sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The Prestige 782R may be referred to as the Prestige, the P782R or the P782 in this manual.

What is xDSL?

A DSL (Digital Subscriber Line) enhances the data capacity of the existing telephone line running between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000Hz to filter noise from the voice line. Several DSL services offer speeds of up to 52 Mbits/sec. DSL services are either symmetrical (traffic flows at the same speed in both directions) or asymmetrical (the downstream capacity is higher than the upstream capacity).

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds for DSL maximum transmission distances. A G.SHDSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

G.SHDSL

G.SHDSL (Single-pair High-speed Digital Subscriber Line) is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire and provides data rates up to 2.3 Mbits/sec. (The "G." in "G.SHDSL" is defined by the G.991.2 ITU (International Telecommunication Union) state-of-the-art industry standard).

The Benefits of G.SHDSL:

- **Continuous Connection** You are always online.
- **Dedicated Bandwidth** Line speed is "symmetric," i.e., the same bandwidth in both directions.
- **Investment Protection** Scalability. Offers a flexible upgrade path. You can choose a higher access speed yourself - no site visit is necessary.
- **Low Maintenance** Connectivity requires no complex manual configuration; G.SHDSL equipment is Plug and Play.
- **Distance Capabilities** G.SHDSL achieves 20% better loop-reach than older versions of symmetric DSL. (Loop reach defines speed that can be attained at various distances).

Part I:

GETTING STARTED

Chapters 1 to 3 guide you through connecting, installing and setting up your Prestige.

Chapter 1

Getting to Know Your G.SHDSL Router

This chapter covers the key features and main applications of your Prestige.

The Prestige 782R Router can be used for high-speed LAN-to-LAN connections or Internet access through a G.SHDSL connection over the telephone line. You can use your Prestige for either IP routing or bridging depending on your ISP (Internet Service Provider) configuration.

1.1 Features of the Prestige

The following features make the Prestige a complete and the flexible networking solution for most users.

High Speed Scalability

One of the best features of G.SHDSL service is its scalability. Your Prestige G.SHDSL router supports symmetrical multi-rate data transmission speeds from 144 Kbps up to 2320 Kbps. You can increase the capacity of the Internet connection (within certain distance limitations) without changing your ISP or purchasing new equipment. G.SHDSL's high symmetrical speeds are ideal for applications like web hosting and videoconferencing as well as the two-way data traffic needs of businesses.

Symmetrical High Speed Internet Access

The Prestige 782R supports symmetrical transmission up to 2.3 Mbps. For NSP's (Network Service Provider) convenience, the Prestige also supports rate management depending on distances and service charges.

SNMP (Simple Network Management Protocol – version 1)

SNMP, a member of the TCP/IP protocol suite, allows you to exchange management information between network devices. Your Prestige supports SNMP agent functionality that allows a manager station to manage and monitor the Prestige through the network.

SNMP is only available if TCP/IP is configured on your Prestige.

IP Multicast

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236). Both versions 1 and 2 are supported by the Prestige.

IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

IP Policy Routing

IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

10/100MB Auto-negotiation Ethernet/Fast Ethernet Interface

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately, providing a faster data transfer on the Ethernet network as required. It enables fast data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Protocols Supported

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP (Point-to-Point Protocol) link layer protocol.
- SUA™ (Single User Account) and NAT (Network Address Translation).

Multiple Protocol Support

- Novell IPX (Internetwork Packet eXchange) network layer protocol.
- Transparent bridging for unsupported network layer protocols.

PAP and CHAP Security

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is available on more platforms.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to other systems that support the DHCP client. The Prestige can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

Data Compression

Your Prestige incorporates Stac LZS data compression ratios of up to 4:1 to speed up data transfer. Stac is the de facto standard of data compression over PPP links.

Encapsulation

The Prestige supports PPP over ATM (RFC-2364), Multiple Protocol over ATM (RFC-1483) and ENET ENCAP.

SUA for Single-IP Address Internet Access

The Prestige's SUA (Single User Account, equivalent to NAT) feature allows multiple user Internet access for the cost of a single ISP account and allows multiple users on the LAN (Local Area Network) to access the Internet concurrently. SUA supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, ICQ, RealAudio, VDOLive, Quake and PPTP. No extra configuration is needed to support these applications. SUA address mapping can also be used for other LAN-to-LAN connections.

Full Network Management

- Menu driven SMT (System Management Terminal) management
- SNMP manageable
- Local SMT session via console port
- Remote SMT session via Telnet

Upgrade Firmware via LAN

In addition to the direct console port connection, the Prestige supports the up/downloading of firmware and configuration file over the LAN.

Filters

The Prestige's packet filtering functions allow added network security and management.

Ease of Installation

Your Prestige is designed for quick, easy and intuitive installation. Its compact size and light weight make it easy to position anywhere in your busy office.

Auxiliary Port

The Prestige has another WAN port as backup in case the xDSL line degrades or is down. For small business and home users, data applications can be more robust and flexible by connecting to an external modem or ISDN TA.

Wall-Mounting

On the underside of the housing are two slots that can be used to wall-mount your Prestige.

1.2 Application Scenarios for the Prestige

1.2.1 Internet Access

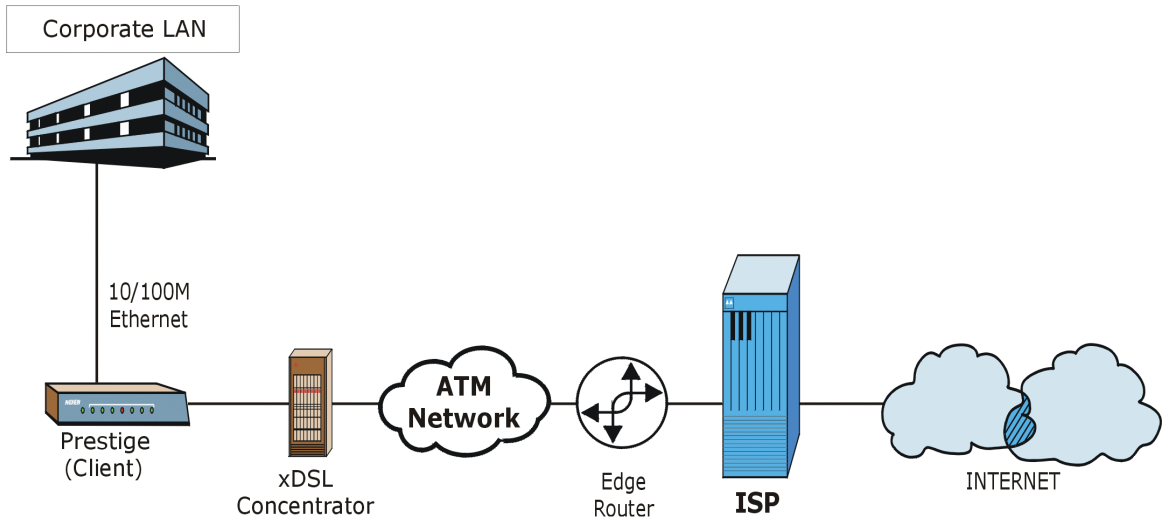


Figure 1-1 Internet Access Application

Your Prestige can act as either of the following:

- An IP/IPX LAN router for a sub-network (Class C or smaller).
- A bridge for multi-computer/MAC bridging (RFC-1483, bridged Ethernet/802.3).

1.2.2 LAN-to-LAN Application

You can use the Prestige to connect two geographically dispersed networks over the DSL line. A typical LAN-to-LAN application is shown next.

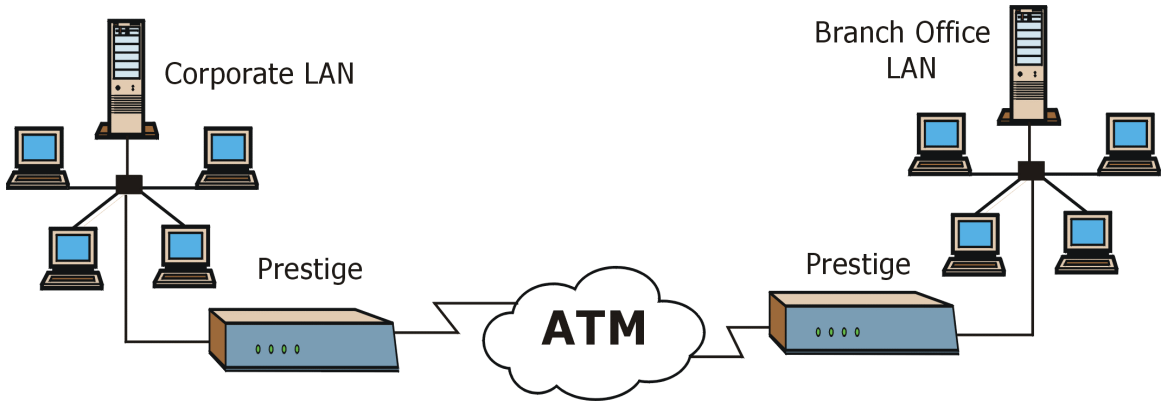


Figure 1-2 LAN-to-LAN Application

Chapter 2

Hardware Installation and Initial Setup

This chapter shows how to make cable connections and set up your xDSL connection using the SMT.

2.1 Installation Requirements

In addition to your Prestige package, your computer should include the following hardware and software:

- An Ethernet 10/100Base-T NIC (Network Interface Card).
- Communications software configured as follows: VT100 terminal emulation; 9600 Baud; No parity, 8 Data bits, 1 Stop bit, no Flow Control.

2.2 Front Panel LEDs of the Prestige 782R

The LED indicators on the front panel show the operational status of the Prestige.

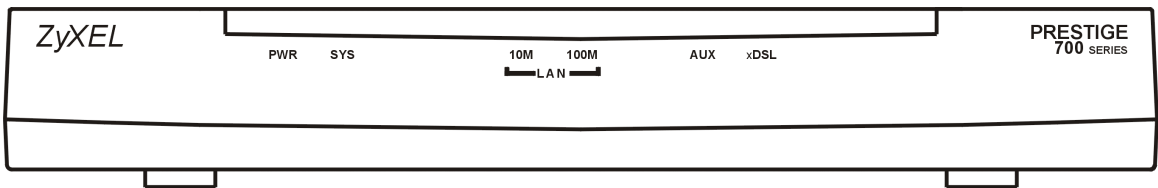


Figure 2-1 Front Panel of Prestige 782R

Table 2-1 LED Functions

LED	COLOR	STATUS	MEANING
PWR	Green	Steady	Your Prestige is on.
SYS	Green	Steady Blinking Off	Your Prestige is on and functioning properly. The system is rebooting, running self-diagnostics or connecting. Your Prestige is not ready or has a malfunction.
LAN 10M	Green	Steady Blinking	You have a successful 10Mb Ethernet connection. Data is being sent or received.

LED	COLOR	STATUS	MEANING
LAN 100M	Orange	Steady Blinking	You have a successful 100Mb Ethernet connection. Data is being sent or received.
AUX	Green	Steady Off	The auxiliary port is connected to the modem or TA. The auxiliary WAN is disconnected.
xDSL	Green	Steady Blinking Blinking Off	Your Prestige is connected to an xDSL line. (2 times per second) - The link is synchronizing - this may take several minutes. (4 times per second) - The link is transmitting and receiving. The Prestige is unplugged or disconnected.

2.3 Rear Panel and Connections of the Prestige 782R

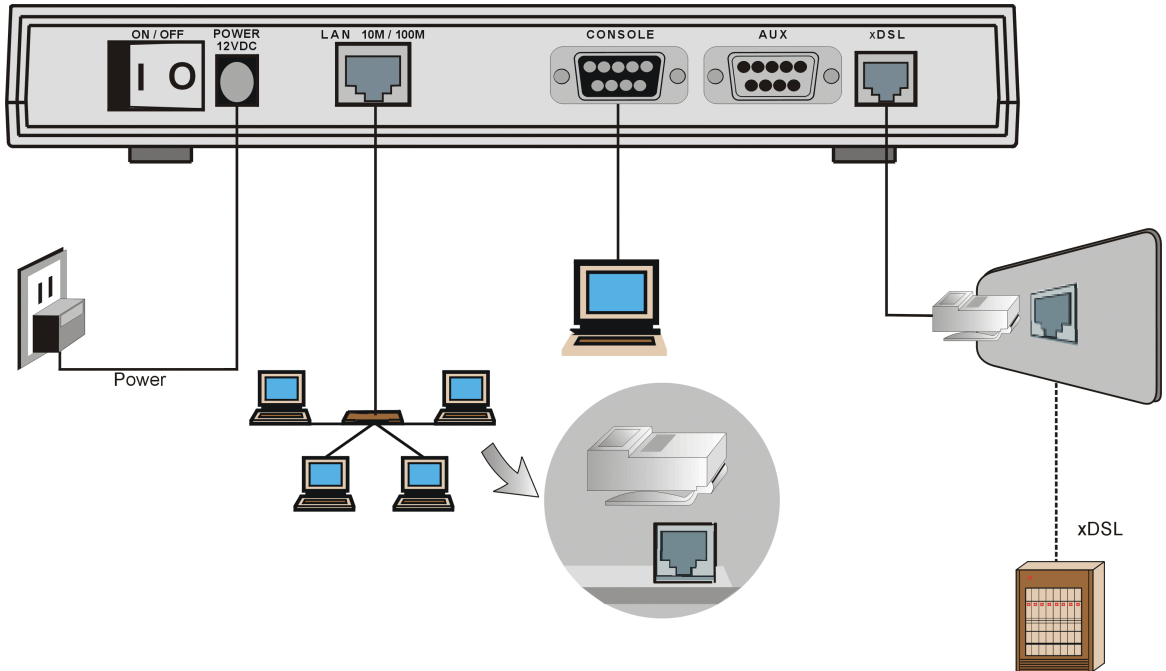


Figure 2-2 Rear Panel of the Prestige 782R

Connecting your Prestige to the LAN and xDSL network.

To prevent damage to the Prestige:
DO NOT connect the G.SHDSL line to the LAN port jack.
DO NOT connect your telephone line to the xDSL RJ-11 port.

Step 1. Connecting the xDSL Line

Plug the Prestige (port labeled xDSL) into the telephone jack using the RJ-11 cable (supplied).

Step 2. Connecting the Console Port

For the initial configuration of your Prestige, you need to use terminal emulator software on a computer and connect it to the Prestige through the console port. Connect the 9-pin end of the console cable to the console port of the Prestige and the other 9-pin end to a serial port (COM1, COM2 or other COM port) of your computer. You can use an extension RS-232C cable if the enclosed one is too short.

Step 3. Connecting a Computer to the Prestige

Ethernet 10Base-T networks use Unshielded Twisted Pair (UTP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. Use the crossover cable to connect your Prestige to a computer directly or use straight-through Ethernet cable to connect to an external hub and then connect one end of the straight-through Ethernet cable from the hub to the NIC on the computer.

Step 4. Connecting the Power Adapter to your Prestige

Connect the power adapter to the port labeled **POWER** on the rear panel of your Prestige.

To prevent damage to the Prestige, first make sure you have the correct DC power adapter specifications for your particular region. (See the Appendix section)

2.4 Turning On Your Prestige

You can now turn on your Prestige by flipping the power switch to the on position (**I** is ON, **O** is OFF).

Step 1. Initial Screen

When you turn on your Prestige, it performs several internal tests as well as line initialization. After the initialization, the Prestige prompts you to press [ENTER] to continue, as shown.

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.  
initialize ch =0, ethernet address: 00:a0:c5:01:23:45  
WAN Channel init.....done  
Press ENTER to continue...
```

Figure 2-3 Power-On Display

Step 2. Entering the Default System Password

The login screen will prompt you to type the password. For your first login, type the default password **1234**. The screen displays an “X” for each character you type.

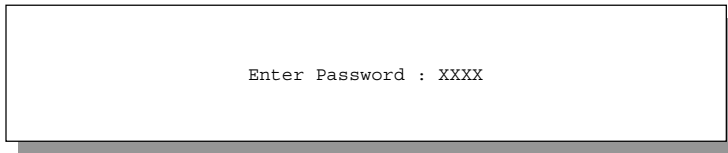


Figure 2-4 Login Screen

If, after logging on, there is no activity for longer than 5 minutes, your Prestige will automatically log you out and display a blank screen. Press [ENTER] to bring up the login screen again.

2.5 Navigating the SMT Interface

You will be using the SMT (System Management Terminal) interface to configure your Prestige. The following figure is an overview of the Prestige SMT menu screens.

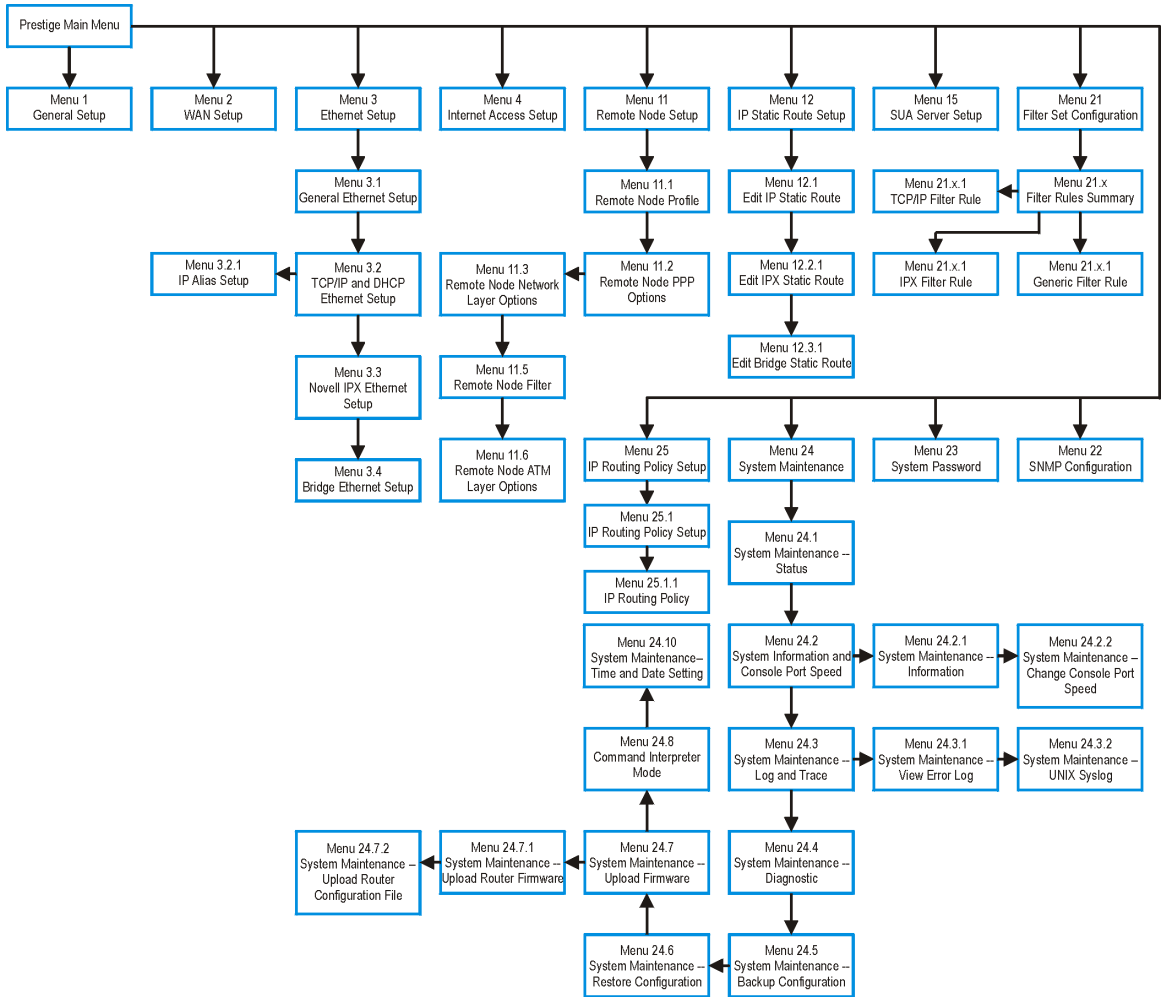


Figure 2-5 Prestige 782R SMT Menu Overview

2.6 SMT Menu Commands

Before changing the configuration, familiarize yourself with the operations listed in the following table.

**You can make future changes to the configuration through telnet connections.
See the *Telnet Configuration and Capabilities* chapter.**

Table 2-2 Main Menu Commands

COMMAND	DESCRIPTION
Move forward to another menu	Type the number of the desired menu and press [ENTER].
Move to a previous menu	Press the [ESC] key to move back to the previous menu.
Move to a submenu	Press [SPACE BAR] to change No to Yes , then press [ENTER] to go to a submenu. (Fields beginning with “Edit” have default setting of No .)
Move the cursor	Press [ENTER] within a menu to move to the following field or use the [Up]/[Down] arrow keys to move to the previous or the following field.
Enter information	Press [SPACE BAR] to cycle through the choices or type the appropriate information in the field.
Save your configuration	Press [ENTER] at the prompt “Press [ENTER] to confirm...”. Saving the screen data will usually take you to the previous menu.
Exit the SMT	Type 99 at the Main Menu and press [ENTER].

**Remember to fill in all required fields (denoted by the symbol [?]).
N/A refers to an option that is Not Applicable.**

After you type the password, the SMT displays the Main Menu, as shown.

```

Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
Prestige 782R   Main Menu

Getting Started
1. General Setup
2. WAN Setup
3. Ethernet Setup
4. Internet Access Setup

Advanced Applications
11. Remote Node Setup
12. Static Routing Setup
15. SUA Server Setup

Advanced Management
21. Filter Set Configuration
22. SNMP Configuration
23. System Password
24. System Maintenance
25. IP Routing Policy Setup

99. Exit

Enter Menu Selection Number:
```

Figure 2-6 SMT Main Menu

2.6.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

No.	MENU TITLE	FUNCTION
1	General Setup	To set up general information.
2	WAN Setup	To set up the WAN.
3	Ethernet Setup	To set up Ethernet.
4	Internet Access Setup	To set up Internet connection.
11	Remote Node Setup	To set up the Remote Node for LAN-to-LAN and Internet connections.
12	Static Routing Setup	To set up static route for different protocols.
15	SUA Setup	To configure SUA.
21	Filter Set Configuration	To set up filters to provide security, call control, etc.
22	SNMP Configuration	To set up SNMP-related parameters.
23	System Password	To set up security-related parameters.
24	System Maintenance	System status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	To set up configuration for routing policies.
99	Exit	To exit from SMT and return to the blank screen.

2.7 Changing the System Password

Change the default system password by performing the following steps.

- Step 1.** In the Main Menu, type **23** to open **Menu 23 – System Password** as shown in the following figure. When the menu appears, type the old system password, i.e., 1234, and press [ENTER].

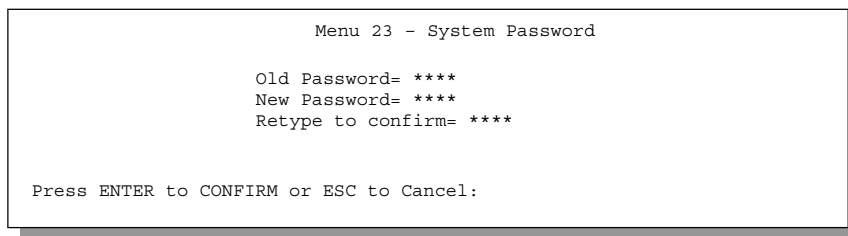


Figure 2-7 Menu 23 – System Password

Step 2. Type your new system password (up to 30 characters) and press [ENTER].

Step 3. Re-type your new system password to confirm and press [ENTER].

The screen displays an asterisk "*" for each character you type.

2.8 Resetting the Prestige

If you forget your password or cannot access the SMT menu, you need to reinstall the configuration file. Reinstallation replaces the current file with the factory configuration file. All custom configurations will be lost and the console port speed will be reset to the default. (9600 bps with 8 data bit, no parity, 1 stop bit (8n1), and no Flow Control.) The password will be reset to the default of 1234.

Turn off your Prestige and begin a Terminal session with the current console port settings. Turn on your Prestige again. You should see the following screen. When you see the message "Press any key to enter debug mode within 3 seconds", press any key. Make sure you have the configuration file or have already downloaded the latest one from the ZyXEL web site.

```
Bootbase Version: V2.00 | 4/14/2000 13:58:03
RAM: Size = 8192 Kbytes
DRAM POST: Testing: 8192K OK
FLASH: Intel 8M *2

ZyNOS Version: V2.50(BH.0)b5 | 12/12/2000 14:01:55

Press any key to enter debug mode within 3 seconds.
.....
(Compressed)
Version: P782R STU, start: 0203c030
Length: 149AA0, Checksum: EEB7
Compressed Length: B4140, Checksum: A562
```

Figure 2-8 Booting Up the Prestige

To upload the configuration file, do the following:

Step 1. Type **atlc** after the **Enter Debug Mode** message.

Step 2. Wait for the **Starting XMODEM upload** message before activating XMODEM upload on your terminal.

Step 3. After a successful firmware upload, type **atgo** to restart the Prestige.

The Prestige is now reinitialized with a default configuration file including the default password of 1234.

2.9 General Setup

Menu 1 – General Setup contains administrative and system-related information.

To go to **Menu 1** and fill in the required information, follow these steps:

Step 1. In the Main Menu, type **1** to open **Menu 1 – General Setup**, shown next.

Step 2. Fill in the required fields marked [?] and turn on the individual protocols for your applications, as explained in the following table.

```

Menu 1 - General Setup

System Name= P782
Location= MyHouse
Contact Person's Name= JohnDoe

Route IP= Yes
Route IPX= No
Bridge= No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 2-9 Menu 1 – General Setup

Table 2-4 General Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
System Name	Type any descriptive name, (with no spaces), up to 30 alphanumeric characters long, including dashes “-” and underscores “_”. This field is for descriptive purposes; however, some ISPs check this name. If your ISP checks this name then you should type your computer’s “Computer Name” (Start -> Settings -> Control Panel Network). Click on the Identification tab and note the entry for the Computer Name field.	P782R
Location (optional)	Type the location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Type the name (up to 30 characters) of the person in charge of your Prestige.	JohnDoe
Route IP	Select Yes to enable IP routing. This is needed to access the Internet.	Yes
Route IPX	Select Yes to enable IPX routing.	No
Bridge	Select Yes to enable bridging (see note on Bridging).	No

2.9.1 Note on Bridging

When bridging is enabled, your Prestige forwards any packet that it does not route. Without bridging, the packets are simply discarded. Bridging generates far more traffic than routing for the same network protocol and consumes more CPU cycles and memory.

The Prestige can also serve as a LAN router. To do this, in Menu 4 choose Encapsulation = ENET ENCAP, with the Single User Account enabled (default). Because there is only one IP address it will be assumed that there is only one computer on the xDSL line.

2.10 Setting Up the WAN Link

Use **Menu 2 – WAN Setup** to configure G.SHDSL settings for your WAN line. Different telephone companies deploy different types of G.SHDSL service. If you are unsure of any of this information, please check with your telephone company.

2.10.1 Service Type

Is your Prestige acting as a Server or Client?

1. The Prestige is a server if it is acting as a COE (Central Office Equipment).
2. The Prestige is a client if it is acting as a CPE (Customer Premise Equipment).

2.10.2 Rate Adaption

Both the Prestige and the peer must have the same transmission rate. Rate Adaption allows the Prestige to auto-detect the peer **Transfer Rate** (this feature may not be available on all models).

2.10.3 Transfer Rates

The Prestige supports the following symmetrical multi-rate data transmission speeds: 144, 200, 208, 272, 392, 400, 528, 776, 784, 1040, 1168, 1552, 2064 and 2320Kbps.

You can increase the capacity of the Internet connection (within certain limitations) without changing your ISP or buying new equipment.

For back-to-back applications make sure that your Prestige and its peer have the same **Transfer Max Rate** and the same **Transfer Min Rate**. Two (maximum and minimum) transfer rates are used to accommodate fluctuations in line speed. This is known as Dynamic Bandwidth Allocation.

2.10.4 Standard Mode

If your Prestige is a server, then select the mode that applies to your region: ANSI (American National Standards Institute) and ETSI (European Telecommunications Standards Institute). If your Prestige is a client, select the same **Standard Mode** that the server side selects. ANSI and ETSI create recommendations and standards for the telecommunications industry.

```

Menu 2 - WAN Setup

Service Type: Client
Rate Adaption= Enable
Transfer Max Rate(Kbps) = 2320K
Transfer Min Rate(Kbps) = 144K
Standard Mode= ANSI (ANNEX_A)

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 2-10 Menu 2 – WAN Setup

Table 2-5 Menu 2 – WAN Setup

FIELD	DESCRIPTION
Service Type	Press [SPACE BAR] to select Server (COE) or Client (CPE).
Rate Adaption	Press [SPACE BAR] to select Enable (activate) or Disable (deactivate).
Transfer Max Rate (2320 Kbps)	Press [SPACE BAR] to select a Transfer Max Rate greater than or equal to the Transfer Min Rate and press [ENTER] to continue.
Transfer Min Rate (144 Kbps)	Press [SPACE BAR] to select a Transfer Min Rate less than or equal to the Transfer Max Rate and press [ENTER] to continue.
Standard Mode	Press [SPACE BAR] to select ANSI (ANNEX A) or ETSI (ANNEX B) and press [ENTER] to continue. The Client side must match the Server side.

2.11 Ethernet Setup

In the Main Menu, type **3** to open **Menu 3 – Ethernet Setup** to configure the Ethernet.


```
Menu 3 - Ethernet Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup
3. Novell IPX Setup
4. Bridge Setup

Enter Menu Selection Number:
```

Figure 2-11 Menu 3 – Ethernet Setup

2.11.1 LAN Setup

Use this menu to specify filter set(s) that you want to apply to Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful for blocking certain packets, reducing traffic and preventing security breaches.

```
Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Press ENTER to Confirm or ESC to Cancel:
```

Figure 2-12 Menu 3.1 – LAN Port Filter Setup

If you need to define filters, please read the chapter *Filter Set Configuration* first, then return to this menu.

2.11.2 Protocol Dependent Ethernet Setup

- To set up TCP/IP Ethernet see the section on *Internet Access Applications*.
- To set up Novell IPX Ethernet see the section on *Ethernet Setup*.
- To set up Bridging Ethernet see the section on *Bridging Setup*.

Chapter 3

Internet Access

This chapter shows how to configure the LAN and WAN for Internet access.

3.1 Ethernet Factory Defaults

The Ethernet parameters of the Prestige are preset in the factory with the following values:

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits).
2. DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for most installations. If the parameters are satisfactory, you can skip to the *TCP/IP Ethernet Setup and DHCP* Section 3.3 to type the DNS server address(es) if your ISP gives you explicit DNS server address(es). To change the factory defaults or to learn more about TCP/IP, please read on.

3.2 TCP/IP and DHCP Ethernet Setup: DHCP

3.2.1 DHCP Setup

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to other systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

3.2.2 Client IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64 for the client computers. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server computers, e.g., server for mail, FTP, telnet, web, etc., that you may have.

3.2.3 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, a user must know the IP address of a computer before can accessing it.

Your ISP may assign you DNS server addresses in an information sheet when you sign up. If so, type them into the **DNS Server** fields in **DHCP Setup**. If you leave this server field set to 0.0.0.0, the Prestige will act as a DNS proxy.

Some ISP's choose to bypass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after connection. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Prestige supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are left as 0.0.0.0, the Prestige tells the DHCP clients that the Prestige is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you type their IP addresses in the **DHCP Setup** menu. This way, the Prestige can pass the DNS servers to the computers and the computers can query the DNS server directly without the Prestige's intervention.

Example of Network Properties for LAN Servers with Fixed IP#

Choose an IP: 192.168.1.2 to 192.168.1.32; 192.168.1.65 to 192.168.1.254.

Netmask: 255.255.255.0

Gateway (or default route): 192.168.1.1 (Prestige LAN IP)

3.2.4 TCP/IP and DHCP Ethernet Setup: TCP/IP

You will now use Menu 3.2 to configure your Prestige for TCP/IP.

3.2.5 IP Address and Subnet Mask

Just as apartments in the same building share a common street address, the computers on a LAN share one common network number.

Where you obtain your network number depends on your particular circumstances. If the ISP or your network administrator assigns you a block of registered IP addresses, follow the instructions in selecting the IP addresses and the subnet mask.

If you have a single user account, the ISP will assign you a dynamic IP address when the connection is established. You must enable the Single User Account feature of the Prestige and choose a network number from 192.168.0.0 to 192.168.255.0. This block of addresses has been reserved for private by The Internet Assigned Number Authority (IANA); please do *not* use any other number.

For example, the IP address 192.168.1.0, covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). The first 3 numbers (192) are the network number while the last number (0) identifies an individual computer on that network.

The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP address that you typed. You do not need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.

Private IP Addresses

Every computer on the Internet must have a unique address. If your networks are isolated from the Internet, e.g., only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, it is recommended that you choose your network number from following three blocks of IP addresses that the Internet Assigned Numbers Authority (IANA) has reserved the specifically for private networks:

10.0.0.0	to	10.255.255.255
172.16.0.0	to	172.31.255.255
192.168.0.0	to	192.168.255.255

Your IP address can be assigned by the IANA, an ISP, or by a private network. Small organizations whose Internet access is through an ISP, will be given Internet addresses for local networks by the ISP. Larger organizations should consult the network administrator for the appropriate IP addresses.

Regardless of your circumstances, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC-1597, *Address Allocation for Private Internets* and RFC-1466, *Guidelines for Management of IP Address Space*.

3.2.6 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to **Both**, the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format. But **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting reduces the load on non-router computers which generally do not listen to the RIP multicast address and so will not receive RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting.

By default, **RIP direction** is set to **Both** and the **Version** set to **RIP-1**.

3.2.7 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender – 1 recipient) or Broadcast (1 sender – everyone on the network). Multicast is a third way to deliver IP packets to selected *group* of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. For more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Prestige supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP Multicasting can be enabled/disabled on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

3.2.8 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT Menu 25 (*see the IP Policy Routing chapter*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

3.2.9 Configuring TCP/IP and DHCP Ethernet Setup

Procedure

- Step 1.** Enable the IP routing in **Menu 1 – General Setup**. To edit **Menu 1**, type **1** in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR] and then press [ENTER].
- Step 2.** To edit Menu 3.2, select the menu option **Ethernet Setup** in the Main Menu. When Menu 3 appears, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**, as shown next.

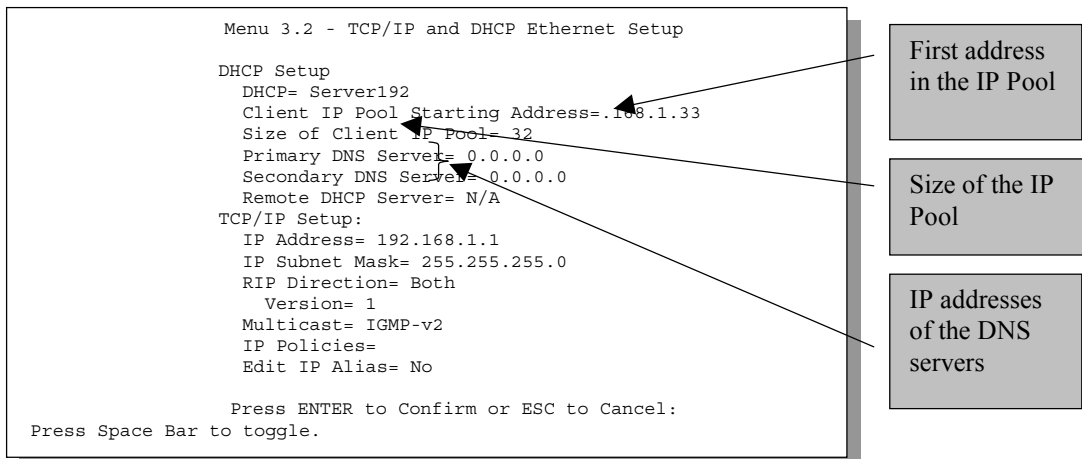


Figure 3-1 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

The following table will show you how to configure the DHCP fields.

Table 3-1 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		
DHCP	This field enables/disables the DHCP server. If set to Server , your Prestige will act as a DHCP server. If set to None , the DHCP server will be disabled. If set to Relay , the Prestige acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to Server , the following four items need to be set:	None Server (default) Relay

FIELD	DESCRIPTION	EXAMPLE
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	32
Primary DNS Server	Type the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Secondary DNS Server		
Remote DHCP Server	If Relay is selected in the DHCP field above, then type the IP address of the actual, remote DHCP server here.	

The following table will show you how to configure the TCP/IP fields.

Table 3-2 TCP/IP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Type the IP address of your Prestige in dotted decimal notation.	192.168.1.1 (default)
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Use the subnet mask computed by the Prestige unless you are implementing subnetting.	255.255.255.0 (default)
RIP Direction	Press [SPACE BAR] to select the RIP Direction from Both/None/In Only/Out Only .	Both (default)
Version	Press [SPACE BAR] to select the RIP version: RIP-1/RIP-2B/RIP-2M .	RIP-1 (default)
Multicast	Turn on/off IGMP support and select the version from IGMP-v2/IGMP-v1/None . This field is disabled if DHCP field is set at Client .	IGMP-v2 (default)
IP Policies	You can apply up to four IP Policy sets (from twelve) by typing their numbers separated by commas, e.g., 3, 4, 6, 11.	3
Edit IP Alias	Please refer to the following section.	
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

3.2.10 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. Through its single physical Ethernet interface the Prestige supports three logical LAN interfaces, acting as the gateway for each.

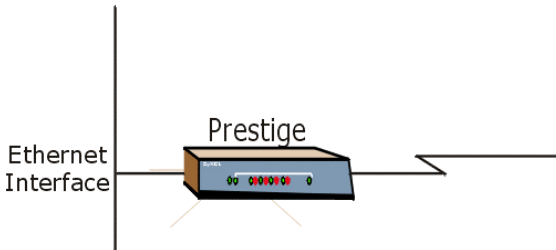


Figure 3-2 Physical Network

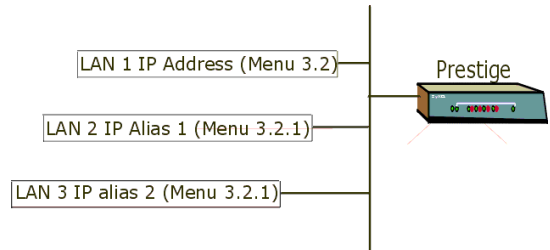


Figure 3-3 Partitioned Logical Networks

Use Menu 3.2.1 to configure IP Alias on your Prestige.

3.2.11 IP Alias Setup

Use **Menu 3.2** to configure the first network and move the cursor to **Edit IP Alias** field and toggle [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to display **Menu 3.2.1 – IP Alias Setup**, as shown next.


```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 3-4 Menu 3.2.1 – IP Alias Setup

Follow the instructions in the following table to configure IP Alias parameters.

Table 3-3 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias 1/2	Choose Yes to configure the LAN network for the Prestige.	Yes
IP Address	Type the IP address of your Prestige in dotted decimal notation.	192.168.2.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select RIP direction from Both/In Only/Out Only .	Both
Version	Press [SPACE BAR] to select from RIP-1/RIP-2B/RIP-2M .	RIP-1
Incoming Protocol Filters	Type the filter set(s) you want to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Type the filter set(s) you want to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

3.3 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand is an outside connection to another network or the Internet.

3.3.1 LANs, WANs and the Prestige

The actual physical connection determines whether the Prestige ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network – the other outside the WAN network as shown next.

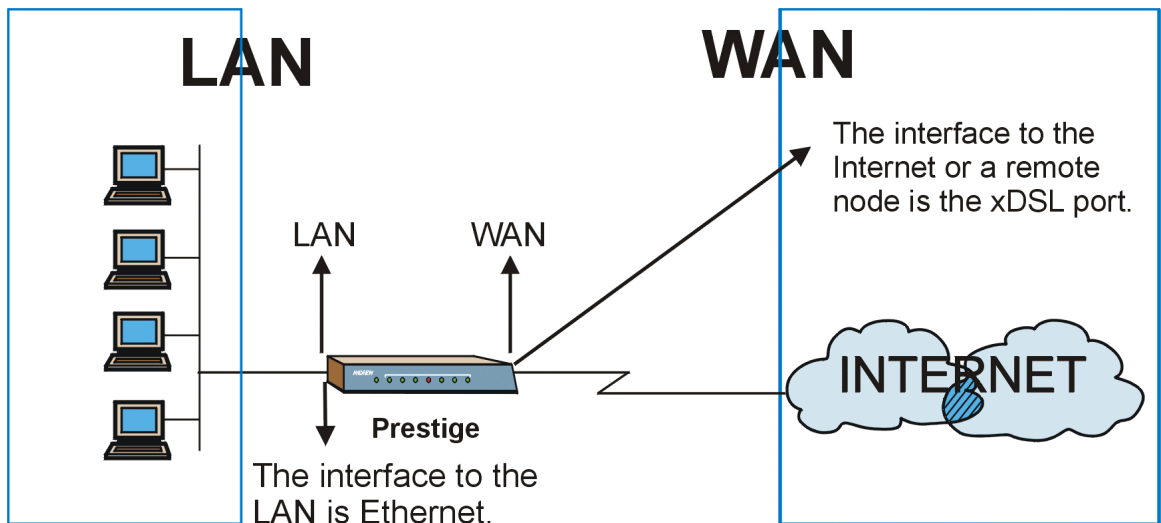


Figure 3-5 LAN and WAN IPs

3.4 Internet Access Configuration

Menu 4 allows you to type the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in Menu 11.

3.4.1 VPI and VCI

Be sure to use the correct VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) numbers supplied by the telephone company. Valid range for VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

3.4.2 Multiplexing

Two conventions are used in identifying what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, e.g., VC1 carries IP, VC2 carries IPX, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large number of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case, one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, e.g., if charging heavily depends on the number of simultaneous VCs.

3.4.3 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods:

PPP

Select this option when the peer is using a “PPP over ATM” networking model. Please refer to RFC-2364 for more information on PPP over ATM Adaptation Layer 5 (AAL5). Refer to RFC-1661 for more information on PPP.

RFC-1483

Select this option when the peer is using a “Multi-protocol over ATM” networking model. RFC-1483 describes two methods for Multi-protocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

ENET ENCAP

The MAC Encapsulated Routing Link Protocol (**ENET ENCAP**) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment, i.e., it encapsulates routed Ethernet frames into bridged ATM cells. **ENET ENCAP** requires that you specify a gateway IP address in the **ENET ENCAP Gateway** field in Menu 4 and in the **Rem IP Addr** field in Menu 11.1. You can obtain this information from your ISP.

3.4.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed. The ISP assigns you a different one each time. The Single User Account (SUA) feature can be enabled or disabled whether you have a dynamic or static IP. However, the encapsulation method assigned influences your choices for IP Address and ENET ENCAP Gateway fields.

Using PPP Encapsulation

If you have a dynamic IP, then the IP Address and **ENET ENCAP Gateway** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the IP Address field and not the **ENET ENCAP Gateway** field.

Using RFC-1483 Encapsulation

In this case the **IP Address Assignment** field must be static with the same requirements for the IP Address and **ENET ENCAP Gateway** fields as stated above for using PPP Encapsulation.

Using ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP, you must fill in all the IP Address and **ENET ENCAP Gateway** fields as supplied by your ISP. However, for a dynamic IP, the Prestige acts as a DHCP client on the WAN port and so the IP Address and **ENET ENCAP Gateway** fields are not applicable (N/A) as they are assigned to the Prestige by the DHCP server.

If you are using PPP encapsulation, then the only ISP information needed is a login name and password. You only need the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

3.4.5 Internet Account Information

Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone company.

Use the following table to record your Internet Account Information.

Table 3-4 Internet Account Information

Internet Account Information	Write your account information here
Telephone Company Information	
VPI (Virtual Path Identifier)	
VCI (Virtual Channel Identifier)	
ISP (Internet Service Provider) Information	
IP Address of the ISP's Gateway (Optional)	
Telephone Number(s) of your ISP	

3.4.6 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the receiver to regulate the average rate and “burstiness” or fluctuation of data transmission over an ATM network. This agreement helps eliminate congestion that is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender is planning to send cells. This parameter may be lower than what the bandwidth of the line permits. 1 ATM cell is 53 bytes (424 bits), so a maximum transfer speed of 2.3Mbps gives a max PCR of 5424 cells/sec. The default value for the Prestige is 5500 cells/sec. This rate is not guaranteed.

Sustained Cell Rate (SCR) is the expected or required cell rate averaged over a long time period. This carrier guarantees this rate as the minimum data transmission rate. SCR may not be greater than the PCR and the Prestige default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that may be sent at the PCR rate in a given time period. The following figure illustrates the relationship between PCR, SCR and MBS.

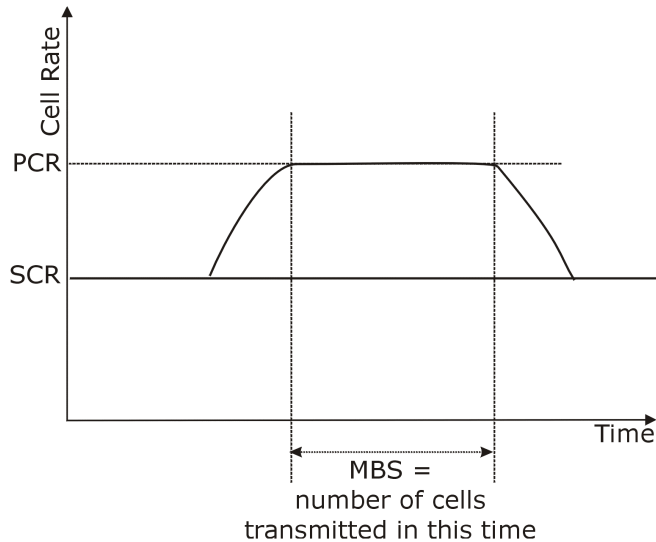


Figure 3-6 Traffic Shaping

3.5 Internet Access Configuration

From the Main Menu, type **4** to display **Menu 4 – Internet Access Setup**, as shown next.

```

Menu 4 - Internet Access Setup

ISP's Name=
Encapsulation= RFC-1483
Multiplexing= LLC-based
VPI #= 0
VCI #= 38
Peak Cell Rate (cell/sec)= 5500
Sustained Cell Rate (cell/sec)= 0
Maximum Burst Size (cell)= 0
My Login= N/A
My Password= N/A
Single User Account= No
IP Address Assignment= Static
IP Address= N/A
ENET ENCAP Gateway= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Get this information from the telephone company. Get the other information from your ISP.

Figure 3-7 Menu 4 – Internet Access Setup

The following table contains instructions on how to configure your Prestige for Internet access.

Table 3-5 Internet Access Setup Menu Fields

FIELD	DESCRIPTION
ISP's Name	Type the name of your ISP, e.g., myISP. This field is for identification purposes only.
Encapsulation	Press [SPACE BAR] to select the method of encapsulation. Options include: PPP (RFC-2364 for PPP over ATM), RFC-1483 (Multi-protocol over ATM) , or ENET ENCAP . If you select ENET ENCAP then the Single User Account field is Yes (enabled) by default.
Multiplexing	Press [SPACE BAR] to select VC-based or LLC-based multiplexing.
VPI #	Type the Virtual Path Identifier (VPI) given by the telephone company.
VCI #	Type the Virtual Channel Identifier (VCI) given by the telephone company.
Peak Cell Rate (cell/sec) Default = 5500 cell/sec	This is the maximum rate at which the sender plans to send cells during the connection's lifetime. NOTE: A 2.3 Mbps line rate will result in a PCR of 5424 cell/sec by setting the Sustained Cell Rate field and Maximum Burst Size field at 0.
Sustained Cell Rate (cell/sec) Default = 0 cell/sec	Sustained Cell Rate, (always smaller than the PCR), is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. Type the SCR, which must be less than the PCR.
Maximum Burst Size (cell)	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
My Login	Type the login name given to you by your ISP.
My Password	Type the password associated with the My Login field above.
Single User Account	Press [SPACE BAR] to enable or disable SUA . Please refer to the section ahead for more details on the Single User Account feature.
IP Address Assignment	Press [SPACE BAR] to select Static or Dynamic address assignment.
IP Address	If your ISP did not assign you a static IP address, type 0.0.0.0; otherwise, type that IP address here. Please refer to the section ahead for more details on setting the IP address under a Single User Account.
ENET ENCAP Gateway	This field is N/A unless you choose ENET ENCAP in the Encapsulation field. Type the gateway IP address supplied by your ISP when applicable.

3.6 Single User Account

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, you will have to lease a block of legal, or globally unique IP addresses from the ISP.

The Single User Account (SUA) feature allows you to have the same benefits as having multiple legal addresses, but only pay for one IP address, thus saving significantly on the subscription fees. (Check with your ISP before you enable this feature). SUA supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake and PPTP with no extra configuration needed.

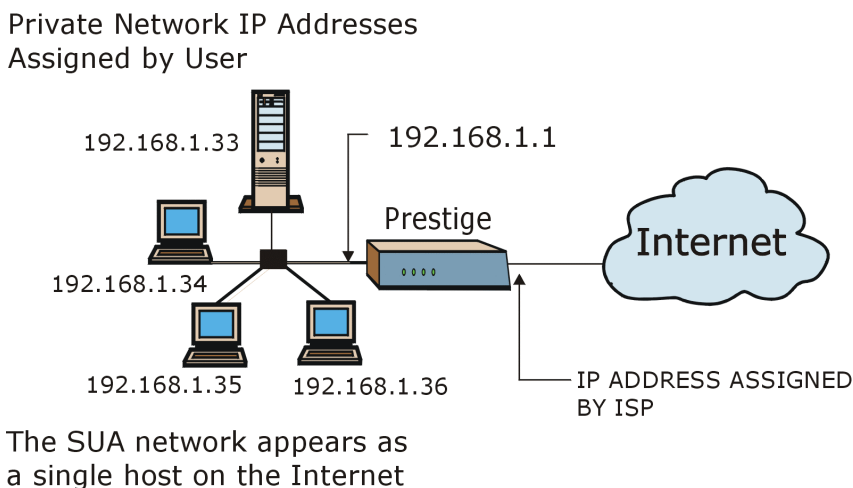


Figure 3-8 Single User Account Topology

The Single User Account feature may also be used on connections to remote networks other than the ISP. For example, this feature can be used to simplify the allocation of IP addresses when connecting branch offices to the corporate network.

The IP address for the SUA can be either fixed or dynamically assigned. In addition, you can designate servers, e.g., a web server on your local network and make them accessible to outside world.

If you do not define any server, SUA offers the additional benefit of firewall protection. If no server is defined, all incoming inquiries will be filtered out by your Prestige and thus preventing intruders from probing your network.

Your Prestige accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC-1631, *The IP Network Address Translator (NAT)*.

3.6.1 Advantages of SUA

- SUA is a cost-effective solution for small offices with less than 20 hosts for accessing the Internet or other remote TCP/IP networks.
- SUA provides firewall protection if no server is specified. All incoming inquiries will be filtered out.
- UDP and TCP datagrams can be routed. Also supported are partial ICMP, echo (ping) and trace route.

3.6.2 Single User Account Configuration

Configuring for Single User Account is the same as for the conventional Internet access except that you need to fill in two extra fields in **Menu 4 – Internet Access Setup**, as shown in the following figure. SUA here is applied solely to the output interface and is valid *only* for LAN – WAN connections and *not* for connections between LANs.

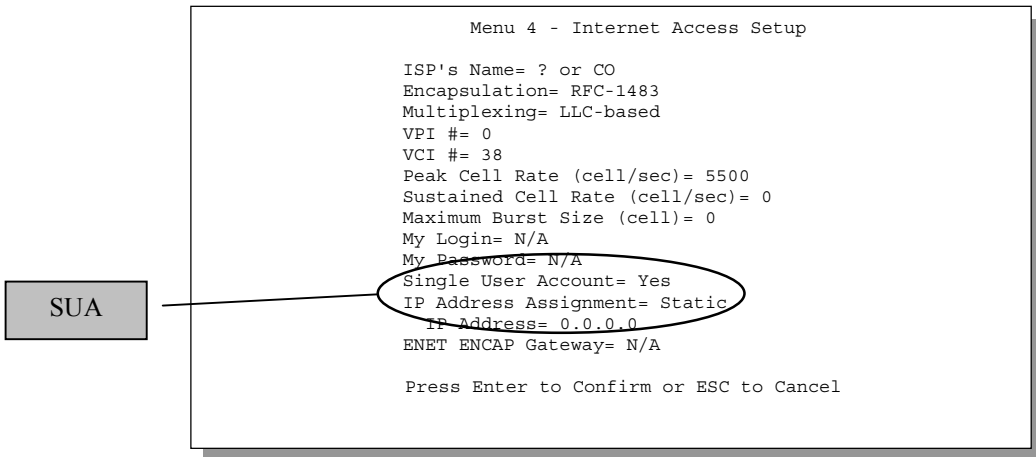


Figure 3-9 Menu 4 – Internet Access Setup for Single User Account

To enable the SUA feature in Menu 4, move the cursor to the **Single User Account** field and select **Yes** (or **No** to disable). Then follow the instructions on how to configure the SUA fields in the following table.

Table 3-6 Single User Account Menu Fields

FIELD	DESCRIPTION
Single User Account	Select Yes to enable SUA .

IP Address	Type the static address assigned by your ISP or type 0.0.0.0.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and return to the previous screen.	

3.7 Multiple Servers Behind the SUA

You can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though SUA makes your whole internal network appear as a single computer to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.

As an example, if you have a web server at 192.168.1.36 and an FTP server at 192.168.1.33, then you need to specify for port 80 (web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service. Also, since you need to specify the IP address of a server in the Prestige, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

To make a server visible to the outside world, specify the port number of the service and the inside IP address of the server in **Menu 15 – SUA Server Setup**.

3.7.1 Configuring a Server Behind the SUA

Do the following steps to configure a server behind SUA:

- Step 1.** Type **15** in the main menu to go to **Menu 15 – SUA Server Setup**.
- Step 2.** Type the service port number in the **Port #** field and the inside IP server address in the **IP Address** field.
- Step 3.** Press [ENTER] at the “Press [ENTER] to confirm...” to save your configuration.

```

Menu 15 - SUA Server Setup

      Port #           IP Address
      -----
1.Default           0.0.0.0
2.21                192.168.1.33
3.23                192.168.1.34
4.25                192.168.1.35
5.80                192.168.1.36
6. 0                0.0.0.0
7. 0                0.0.0.0
8. 0                0.0.0.0
9. 0                0.0.0.0
10. 0               0.0.0.0
11. 0               0.0.0.0
12. 0               0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

Figure 3-10 SUA Server Configuration

The most often used port numbers are shown in the following table. See RFC-1700 for more information.

Table 3-7 Services and Corresponding Port Numbers

PORT NUMBER	SERVICES
21	FTP (File Transfer Protocol)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name System)
80	HTTP (Hyper Text Transfer Protocol or WWW)
1723	PPTP (Point-to-Point Tunneling Protocol)

Part II:

ADVANCED APPLICATIONS

Chapters 4 to 7 show how to configure Remote Node, Remote Node TCP/IP, IPX and Bridging.

Chapter 4

Remote Node Configuration

This chapter covers the parameters that are protocol-independent. The protocol-dependent configuration (TPP/IP, IPX and Bridging) is covered in the next chapters.

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use Menu 4 to set up Internet access, you are configuring one of the remote nodes.

4.1 Remote Node Setup

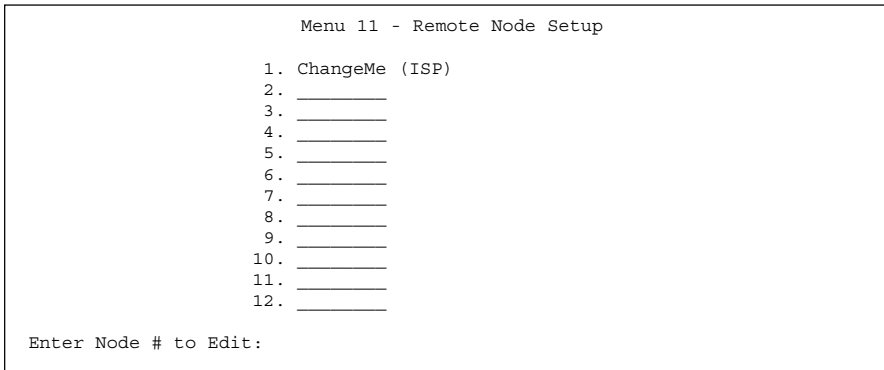
This section describes the protocol-independent parameters for a remote node.

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1. From the Main Menu, select menu option **11 Remote Node Setup**.

Step 2. When Menu 11 appears as shown in the following figure, type the number of the remote node that you want to configure.



```
Menu 11 - Remote Node Setup

1. ChangeMe (ISP)
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____

Enter Node # to Edit:
```

Figure 4-1 Menu 11 – Remote Node Setup

4.1.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. For LAN-to-LAN applications, e.g., branch office and corporate headquarters, prior agreement on methods is necessary because encapsulation and multiplexing cannot be automatically determined. Which methods to use depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entail makes them a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scenario 1. One VC, Multiple Protocols

PPP (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

Scenario 2. One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPP** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

Scenario 3. Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

```
Menu 11.1 - Remote Node Profile

Rem Node Name= nodename          Route= IP
Active= Yes                       Bridge= No

Encapsulation= RFC-1483          Edit PPP Options= No
Multiplexing= LLC-based          Rem IP Addr= 0.0.0.0
Incoming:                        Edit IP/IPX/Bridge= No
  Rem Login= N/A                 Edit ATM Options= No
  Rem Password= N/A
Outgoing:                          Session Options:
  My Login= N/A                  Edit Filter Sets= No
  My Password= N/A
  Authen= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 4-2 Menu 11.1 – Remote Node Profile

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 4-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	OPTIONS
Rem Node Name	[?] denotes a required field. Type a unique, descriptive name of up to eight characters for this node, for example, Plotzer.	
Active	Press [SPACE BAR] to toggle between Yes and No . Inactive nodes are displayed with a minus sign (–).	Yes/No
Encapsulation	PPP refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) of ENET ENCAP are selected, then the Rem Login , Rem Password , My Login , My Password , Edit PPP Options and Authen fields are not applicable (N/A). Moreover, ENET ENCAP encapsulation does not apply to IPX routing.	PPP RFC-1483 ENET ENCAP
Incoming: Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the Rem Password will be used to authenticate this node.	
Rem Password	Type the password used when this remote node calls your Prestige.	
Outgoing: My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: CHAP/PAP – Your Prestige will accept either CHAP or PAP when requested by this remote node. CHAP – accept CHAP (Challenge Handshake Authentication Protocol) only. PAP – accept PAP (Password Authentication Protocol) only.	CHAP/PAP CHAP PAP
Route	This field determines the protocol used in routing.	IP / IPX / IP+IPX / None

FIELD	DESCRIPTION	OPTIONS
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.	Yes/No
Edit PPP Options	To edit the PPP options, move the cursor to this field. Use [SPACE BAR] to select Yes and press [ENTER]. This will take you to Menu 11.2 – Remote Node PPP Options . For more information on configuring PPP options, see the section <i>Editing PPP Options</i> .	Yes
Rem IP Addr	This is a required field if Route is set to IP . Type the IP address of the remote gateway.	192.168.10.1 (example)
Edit IP/IPX/Bridge	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.3 – Remote Node Network Layer Options .	No/Yes
Edit ATM Options	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.6 – Remote Node ATM Layer Options.	No/Yes
Session Options Edit Filter Sets	Use [SPACE BAR] to choose Yes and press [ENTER] to open Menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	No (default)
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.1.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendor’s implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

4.1.4 Editing PPP Options

To edit the remote node PPP options, move the cursor to the **Edit PPP Options** field in **Menu 11.1 – Remote Node Profile**, and use [SPACE BAR] to select **Yes**. Press [ENTER] to open Menu 11.2, as shown next.


```

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No

Enter here to CONFIRM or ESC to CANCEL:

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 4-3 Menu 11.2 – Remote Node PPP Options

The following table describes the Remote Node PPP Options menu and how to configure the PPP options.

Table 4-2 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	OPTIONS
Encapsulation	Select Standard PPP . Select CISCO PPP only if the node is a Cisco computer.	Standard PPP CISCO PPP
Compression	Turn on/off Stac Compression. The default is No .	Yes/No
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.2 Remote Node Setup

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

- Step 1.** In Menu 11.1, make sure **IP** is among the protocols in the **Route** field. The **Route** field should display **IP** or **IP+IPX**.
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, press [SPACE BAR] to toggle and set the value to **Yes**, then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
Single User Account= No
Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies=

IPX Options:
Rem LAN Net #= N/A
My WAN Net #= N/A
Hop Count= N/A
Tick Count= N/A

Bridge Options:
Ethernet Addr Timeout (min)= 0

Press ENTER to Confirm or ESC to Cancel:
    
```

Figure 4-4 Remote Node Network Layer Options

The next table shows you how to configure remote node network layer options.

Table 4-3 TCP/IP-related Fields in Menu 11.1 – Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Route	Make sure IP is among the protocols in this field.	
Rem IP Addr	Type the remote gateway IP address in Remote Node Profile. For a valid IP address, fill in either the remote Prestige WAN IP address or the remote Prestige LAN IP address depending on the remote WAN IP settings. For example, if the remote WAN IP is set at 192.168.3.1, then type 192.168.3.1 in the Rem IP Addr field. If the remote WAN IP is 0.0.0.0, then type 192.168.1.1 in the Rem IP Addr field.	
Edit IP/IPX/ Bridge	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.3 – Remote Node Network Layer Options menu.	Yes/No

The next table explains TCP/IP-related fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 4-4 Remote Node TCP/IP Configuration

FIELD	DESCRIPTION	OPTIONS
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: This is your local Prestige address, not the remote router's.	
Single User Account	Use [SPACE BAR] to toggle between Yes and No . Yes enables the Single User Account feature of your Prestige.	Yes/No
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	1 to 15
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	Yes/No
RIP Direction	Press [SPACE BAR] to select the RIP Direction from Both/In Only/Out Only and None .	Both/None/ In Only/ Out Only
Version	Press [SPACE BAR] to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-1 / RIP-2B / RIP-2M
Multicast	Sets IGMP to version 1, version 2, or disables IGMP.	IGMP-v1/ IGMP-v2/ None
IP Policies	You can apply up to four IP Policy sets (from twelve) by typing in their numbers separated by commas.	3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

4.3 Remote Node Filter

Move the cursor to the field Edit Filter Sets in Menu 11.1, then press [SPACE BAR] to toggle and set the value to **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, e.g., 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets (call protocol filter = 1). Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Figure 4-5 Menu 11.5 – Remote Node Filter

Chapter 5

Remote Node TCP/IP Configuration

This chapter shows a sample LAN-to-LAN application and how to configure TCP/IP remote node.

5.1 TCP/IP Configuration

The following sections describe how to configure the TCP/IP parameters of a remote node.

5.1.1 Editing TCP/IP Options

Follow the steps ahead to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In Menu 11.1, move the cursor to the **Edit ATM Options**, then press [SPACE BAR] to toggle and set the value to **Yes**. Press [ENTER] to open **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of Menu 11.6 for the Prestige , depending on whether you chose **VC-based** or **LLC-based** multiplexing and **PPP** encapsulation in Menu 11.1.

VC-based Multiplexing

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, e.g., VC1 will carry IP, VC2 will carry IPX, etc. Separate VPI and VCI numbers must be specified for each protocol.

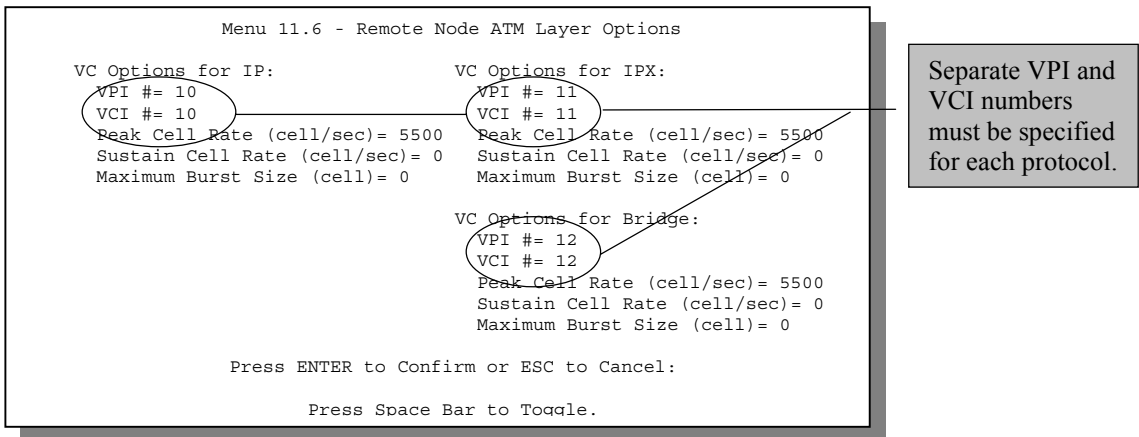
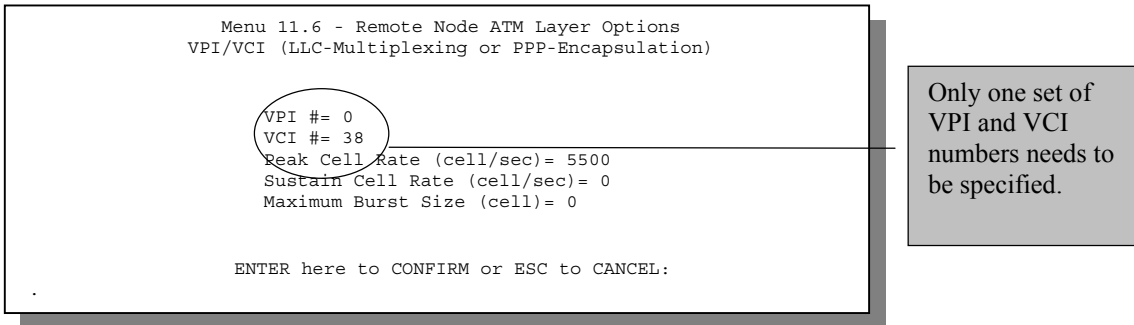


Figure 5-1 Menu 11.6 for VC-based Multiplexing

LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.



The image shows a terminal window for Menu 11.6 - Remote Node ATM Layer Options. The text displayed is:

```
Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

VPI #= 0
VCI #= 38
Peak Cell Rate (cell/sec)= 5500
Sustain Cell Rate (cell/sec)= 0
Maximum Burst Size (cell)= 0

ENTER here to CONFIRM or ESC to CANCEL:
.
```

In the screenshot, the values 'VPI #= 0' and 'VCI #= 38' are circled in black. A grey callout box on the right side of the terminal window contains the text: 'Only one set of VPI and VCI numbers needs to be specified.'

Figure 5-2 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

The following diagram explains the sample IP addresses to help you understand the field of **My Wan Addr** in Menu 11.3. Refer to a previous figure “LAN and WAN IPs” for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Addr** indicates the peer WAN IP.

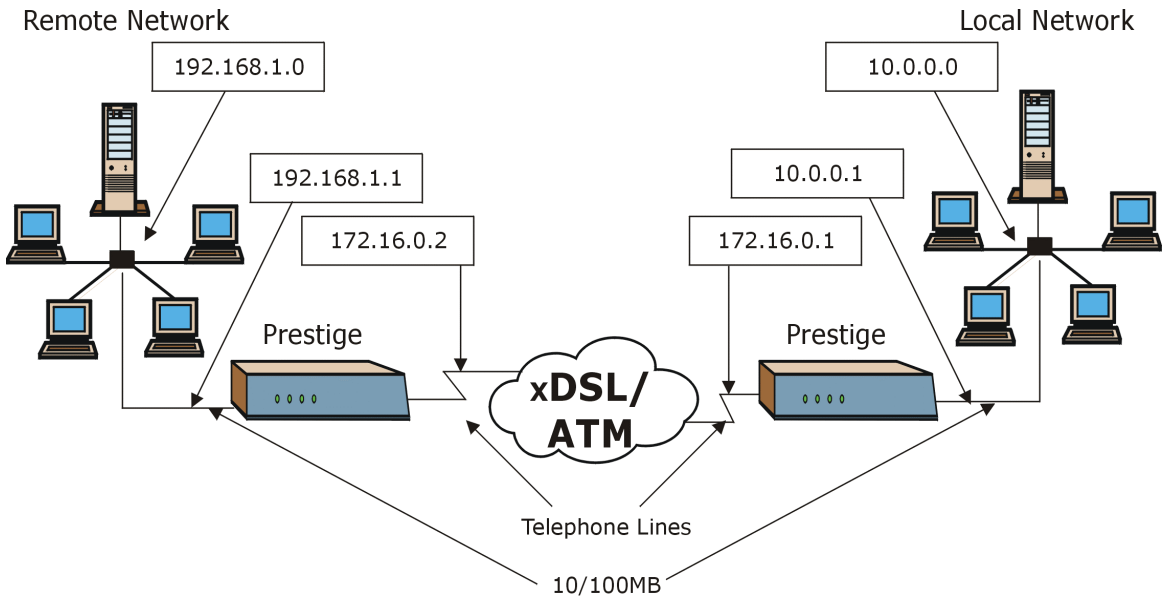


Figure 5-3 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the three fields in **Menu 11.1 – Remote Node Profile**, as shown in the following table. For more details on the IP Option fields, refer to **Chapter 3 – Internet Access Application**.

Table 5-1 TCP/IP-related Fields in Remote Node Profile

FIELD	DESCRIPTION	OPTIONS
Route	Make sure IP is among the protocols in the Route field in Menu 11.1 – Remote Node Profile .	IP
Rem IP Addr	Type the IP address of the remote gateway in Menu 11.1 – Remote Node Profile . Type the remote Prestige’s WAN IP address here (172.12.02 in the example shown previously). If the remote Prestige’s WAN IP address is 0.0.0.0, then type 192.168.1.1 (its LAN IP address) here.	
Edit IP	Press [SPACE BAR] to select Yes and press [ENTER] to display menu.	Yes/No

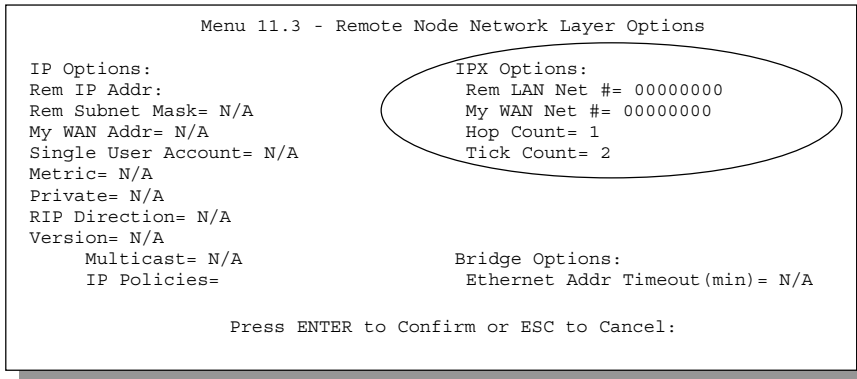


Figure 5-4 Menu 11.3 – Remote Node Novell IPX Options

The following table shows the fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	OPTIONS
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask for the remote network.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: This is the address assigned to your local Prestige, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige Rem IP Addr in Menu 11.1.	
Single User Account	Set this field to Yes to enable the Single User Account feature for your Prestige. Use [SPACE BAR] to choose between Yes and No . See the <i>Internet Access</i> chapter for more information on the Single User Account feature.	Yes/No
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	1 to 15

FIELD	DESCRIPTION	OPTIONS
Private	This decides if the Prestige RIP broadcasts will include the route to this remote node. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	Yes/No
RIP Direction	Press [SPACE BAR] to select from Both/In Only/Out Only/None .	None (default)
Version	Press [SPACE BAR] to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-2B (default)
Multicast	Sets IGMP to version 1, version 2, or disables IGMP.	IGMP-v1/IGMP-v2/None (default)
IP Policies	You can apply up to 4 IP Policy sets (from twelve) by typing their numbers separated by commas.	e.g. 3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

5.1.2 IP Static Route Setup

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following diagram through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

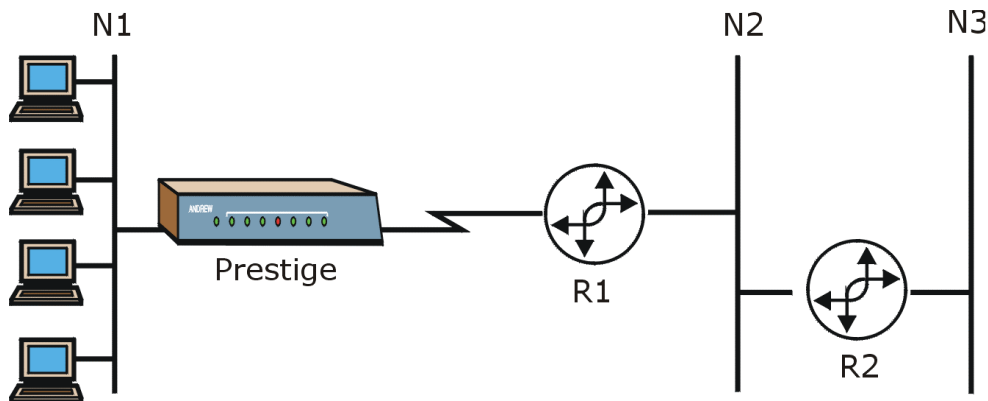


Figure 5-5 Sample Static Routing Topology

To configure an IP static route, use **Menu 12 – Static Route Setup**, as displayed next.

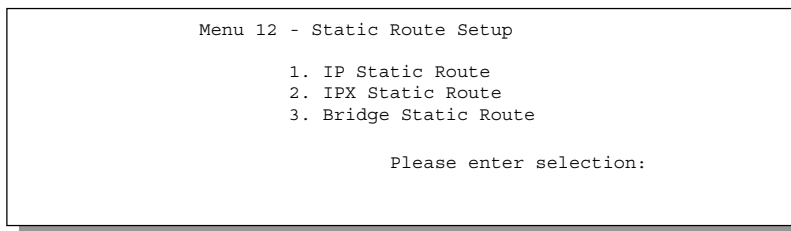


Figure 5-6 Menu 12 – Static Route Setup

From Menu 12, select **1** to open **Menu 12.1 – IP Static Route Setup**, as shown next.

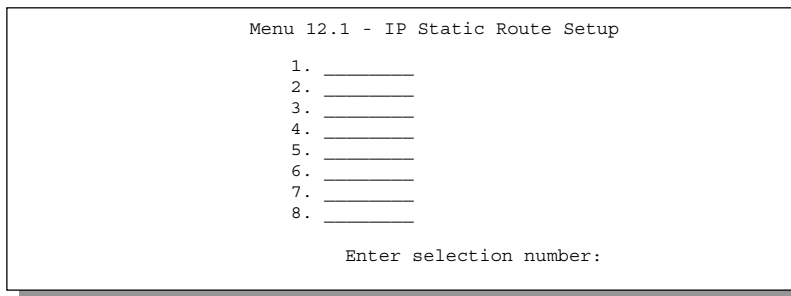


Figure 5-7 Menu 12.1 – IP Static Route Setup

Now, type the index number of one of the static routes you want to configure.

```

Menu 12.1.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 5-8 Edit IP Static Route

The following table describes the fields for **Menu 12.1 – Edit IP Static Route Setup**.

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in Menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on IP subnet mask in this chapter.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

FIELD	DESCRIPTION
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and is not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 6

IPX Configuration

This chapter shows you how to configure the IPX parameters of the Prestige.

6.1 IPX Network Environment

Novell bundles the protocol stack, the server software and routing functionality in their NetWare server products. So a NetWare server is not only a file or print server, it is also a router.

6.1.1 Network and Node Number

Every IPX computer has a network number and a node number, together they form the complete address of the computer. The IPX network number is a 32-bit quantity and is usually expressed in 8 hexadecimal digits, e.g., 0893A8CF. The host number is a 48-bit quantity and usually is taken from the MAC (Media Access Control) address of the Ethernet hardware, so you do not have to explicitly configure the node number.

An IPX client obtains its network number from a server that has the network numbers statically configured. If there are multiple servers on a network, only one server need to have the network numbers configured and all other stations (clients and servers) can obtain the network numbers from it. The server with configured network numbers is called a seed router.

If you have a NetWare server on the same LAN as the Prestige 782 , we recommend that you set up a NetWare server as a seed router. Even though the Prestige is capable as a seed router, a NetWare server offers a much more extensive facility for network management.

6.1.2 Frame Types

IPX can run on top of four different frame types on the Ethernet. These frame types are 802.2, 802.3, Ethernet II (DIX) and SNAP (Sub-Network Access Protocol). Each frame type is a separate logical network, even though they exist on one physical network (see the following diagram).

Even though there are 4 frame types available on the Ethernet, you should configure as few frame types as possible on your NetWare server and use automatic frame detection on the clients to simplify management and to reduce network overhead.

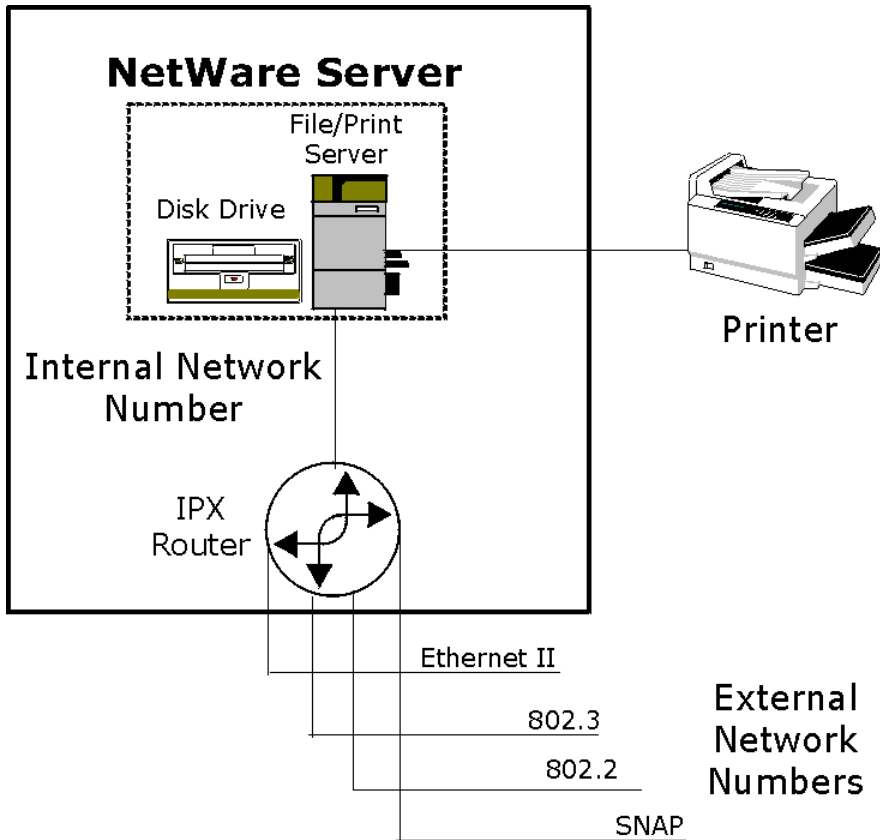


Figure 6-1 NetWare Network Numbers

6.1.3 External Network Number

Each of the 4 logical networks (based on frame type) has its own external network number.

6.1.4 Internal Network Number

In addition to the external network numbers, each NetWare server has its own internal network number that is a virtual network to which the server is attached. It is important to remember that every network number must be unique for that entire network, both internal or external.

6.2 The Prestige in an IPX Environment

There are two scenarios in which your Prestige 782R is deployed, depending on whether there is a NetWare server on the LAN or not, as depicted in the following diagram.

- LAN with a server (server side)
- LAN without a server (client side)

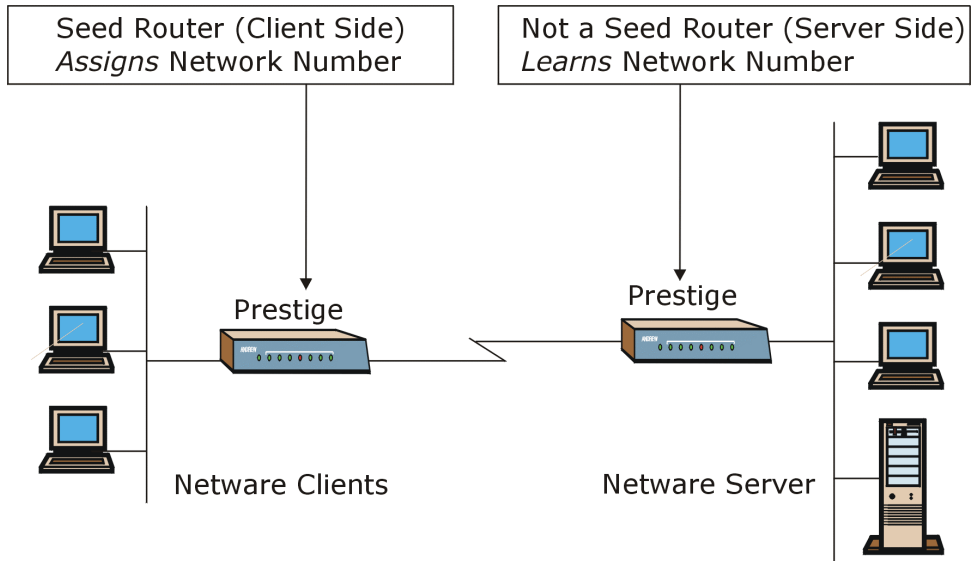


Figure 6-2 Prestige in an IPX Environment

6.2.1 The Prestige on a LAN with a Server

If your Prestige is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige will learn the network number from the seed router and add the routes to its routing table.

6.2.2 The Prestige on a LAN without Server

Each IPX network must have a seed router. If you only have NetWare clients on your network, then you must configure the Prestige as a seed router and set up unique network numbers for each frame type enabled using **Menu 3 – Ethernet Setup** menu.

6.3 IPX Ethernet Setup

From **Menu 3 – Ethernet Setup**, select option **3** to display **Menu 3.3 – Novell IPX Ethernet Setup** as shown in the following example.

```

Menu 3.3 - Novell IPX Ethernet Setup

Seed Router= No

Frame Type 802.2= Yes
  IPX Network #= N/A

Frame Type 802.3= No
  IPX Network #= N/A

Frame Type Ethernet II= No
  IPX Network #= N/A

Frame Type SNAP= No
  IPX Network #= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
    
```

Figure 6-3 Menu 3.3 – Novell IPX Ethernet Setup

The following table describes the Novell IPX Ethernet Setup menu.

Table 6-1 Novell IPX Ethernet Setup Fields

FIELD	DESCRIPTION	OPTIONS
Seed Router	Determines if your Prestige is to act as a seed router.	Yes/No
Frame Type	Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network.	802.2/802.3/ Ethernet II/ SNAP
IPX Network #	If your Prestige is a seed router, type a unique network number for each frame type enabled.	
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

6.4 LAN-to-LAN Application With Novell IPX

A typical LAN-to-LAN application enables the stations in a branch office to access the NetWare servers at Corporate headquarters as depicted in the following example.

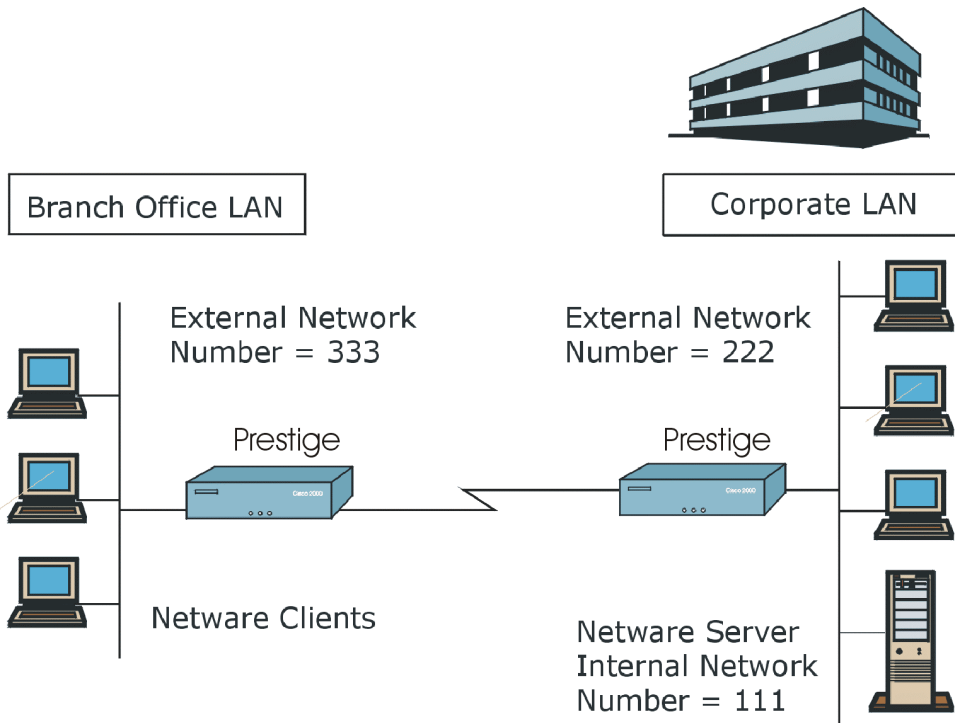


Figure 6-4 LAN-to-LAN Application With Novell IPX

6.4.1 IPX Remote Node Setup

For the IPX-related parameters in **Menu 11.3 – Remote Node Network Layer Options**, perform the following instructions:

- Step 1.** In Menu 11.1, make sure **IPX** is among the protocols in the **Route** field. (The **Route** field should display **IPX**).
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

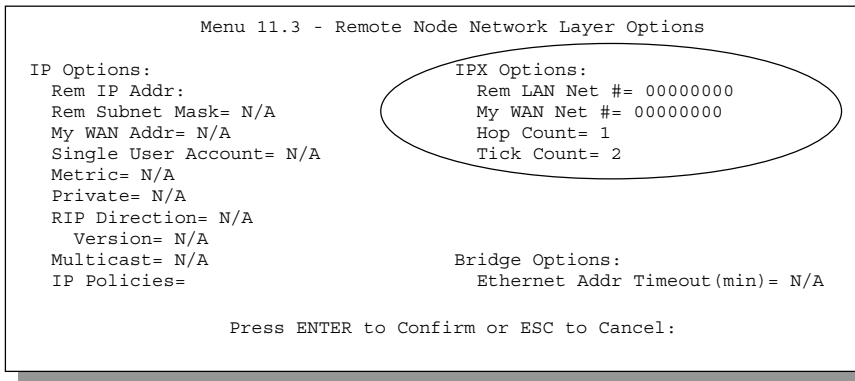


Figure 6-5 Menu 11.3 – Remote Node Novell IPX Options

Table 6-2 Remote Node Novell IPX Options

FIELD	DESCRIPTION	OPTIONS
Rem LAN Net #	Type the internal network number of the NetWare server on the remote LAN.	
My WAN Net #	Type the WAN link network number. If left as 00000000, your Prestige will automatically determine the network number through negotiation with the PPP peer.	00000000 (default)
Hop Count	This is the number of intermediate networks that must be passed through to reach the remote node.	1 (default)
Tick Count	This is the time-ticks required to reach the remote node.	2 (default)
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

6.4.2 IPX Static Route Setup

Similar to IP, IPX static routes tell the Prestige how to reach servers beyond a remote node before a connection to that remote node is established.

From Menu 12, type **2**, then select one of the IPX Static Routes to open **Menu 12.2.1 – Edit IPX Static Route**, as shown next.

```

Menu 12.2.1 - Edit IPX Static Route

Route #= 1
Server Name= ?
Active= Yes
Network #= ?
Node #= 000000000001
Socket #= 0451
Type #= 0004
Hop Count= 2
Tick Count= 3
Gateway Node= 1

Press ENTER to Confirm or ESC to Cancel:

```

Figure 6-6 Menu 12.2.1 – Edit IPX Static Route

The following table contains the instructions on how to configure the Edit IPX Static Route menu.

Table 6-3 Edit IPX Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the route index number as listed in Menu 12.2 – IPX Static Route Setup .
Server Name	Type the server name. This must be the <i>exact</i> name configured in the NetWare server.
Active	This allows you to activate/deactivate this static route.
Network #	This is the internal network number of the remote server you want to access. [00000000] and [FFFFFFFF] are reserved.
Node #	This is the address of the node on which the server resides. For a Novell IPX implementation, the value is [000000000001] .
Socket #	The server will receive service requests on this socket. The default is hex [0451] .
Type #	This identifies the type of service the server provides. The default is hex [0004] .
Hop Count	This is the number of intermediate networks that must be passed through to reach the remote node.
Tick Count	This indicates the time-ticks required to reach the remote node.
Gateway Node	Type the remote node number that is the gateway for this static route.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 7

Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

7.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, e.g., SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reason, do *not* turn on bridging unless you need to support protocols other than IP and IPX on your network. For IP and IPX, enable the respective routing if you need it; do not bridge what the Prestige can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN, however, your Prestige applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the **Handle IPX** field.

From **Menu 3 – Ethernet Setup**, type **4** to enter **Bridge Setup** as shown next.

```
Menu 3.4 - Bridge Ethernet Setup
Handle IPX= None

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 7-1 Menu 3.4 – Bridge Ethernet Setup

The following table describes how to configure the **Handle IPX** field in Menu 3.4.

Table 7-1 Bridge Ethernet Setup Menu – Handle IPX Field Configuration

OPTIONS	DESCRIPTION
None	When no IPX traffic is on the LAN or when you do not want any special handling for IPX.
Client	When only client workstations are on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.
Server	When only IPX servers are on the LAN. No RIP or SAP packets will trigger calls. Also, when the line is down, your Prestige will reply to watchdog messages from the servers on behalf of remote clients. How long your Prestige will do this is linked to the Ethernet Address Timeout parameter in each remote node (see Remote Node Configuration). When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

7.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:

- Step 1.** In Menu 11.1, make sure the **Bridge** field is set to **Yes**.
- Step 2.** Move the cursor to the **Edit IP/IPX/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:
  Rem IP Addr:
  Rem Subnet Mask= N/A
  My WAN Addr= N/A
  Single User Account= N/A
  Metric= N/A
  Private= N/A
  RIP Direction= N/A
  Version= N/A
  Multicast= IP Policies=

IPX Options:
  Rem LAN Net #= N/A
  My WAN Net #= N/A
  Hop Count= N/A
  Tick Count= N/A

Bridge Options:
  Ethernet Addr Timeout (min)= 0

Enter here to Confirm or ESC to CANCEL:

```

Figure 7-2 Menu 11.3 – Remote Node Bridging Options

Table 7-2 Remote Node Bridge Options

FIELD	DESCRIPTION
Bridge (Menu 11.1)	Make sure this field is set to Yes .
Edit IP/IPX/Bridge (Menu 11.1)	Press [SPACE BAR] to change it to Yes and press [ENTER] to display the Remote Node Network Layer Options menu.
Ethernet Addr Timeout (min.) (Menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

7.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in Menu 12.3.1 (go to Menu 12, choose option 3, then choose a static route to edit) as shown next.

```

Menu 12.3.1 - Edit Bridge Static Route

Route #: 1
Route Name=
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

Press ENTER to Confirm or ESC to Cancel:

```

Figure 7-3 Menu 12.3.1 – Edit Bridge Static Route

The following table describes the **Edit Bridge Static Route** menu.

Table 7-3 Edit Bridge Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the route index number as listed in Menu 12.3 – Bridge Static Route Setup .
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active or not.
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Type the number of the remote node that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Part III:

ADVANCED MANAGEMENT

Chapters 8 to 11 discuss Filtering, SNMP, System Maintenance and IP Routing Policy.

Chapter 8

Filter Configuration

This chapter shows you how to create and apply filters.

8.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, e.g., RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

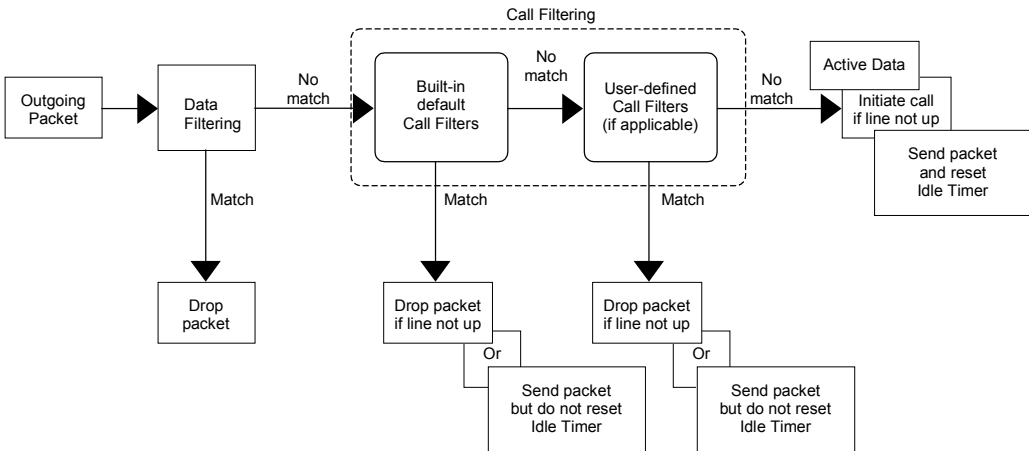


Figure 8-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

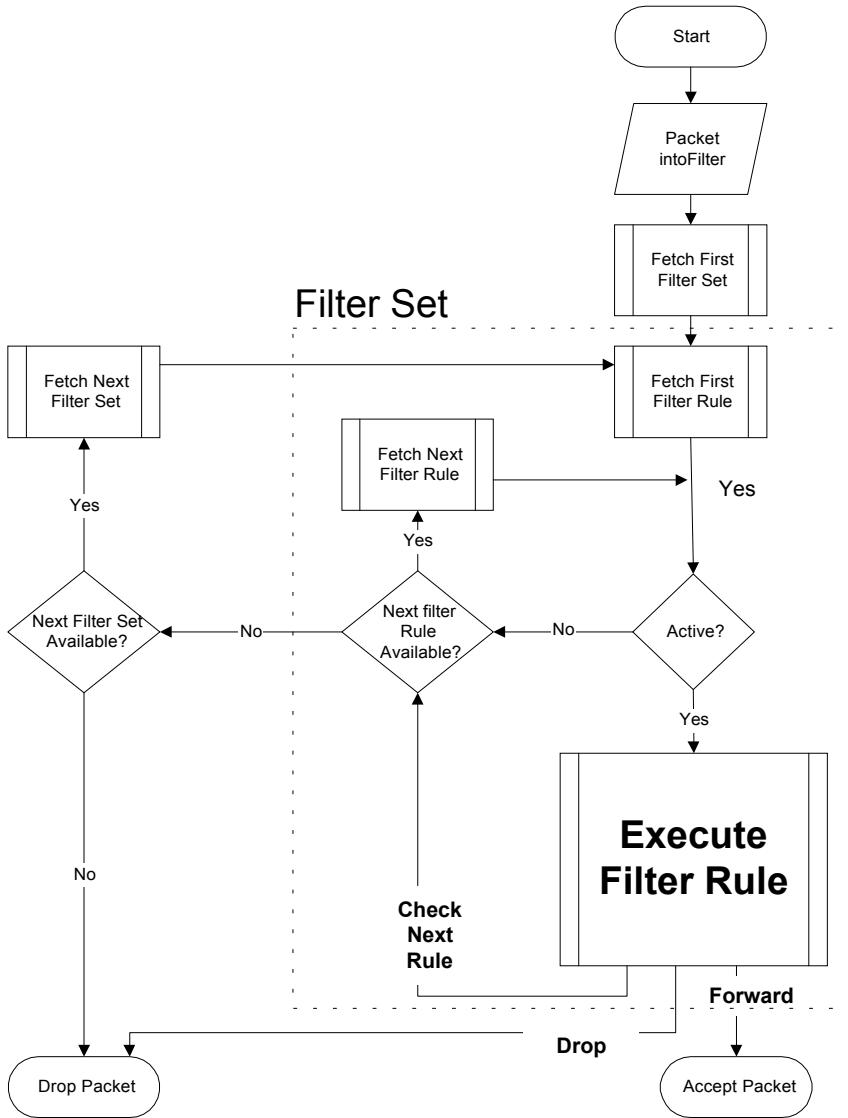


Figure 8-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

You can apply up to 4 filter sets to a particular port to block multiple types of packets. Because each filter set can have up to 6 rules, you can have a maximum of 24 rules active for a single port.

8.2 Configuring a Filter Set

To configure a filter set, follow the procedures indicated:

Step 1. Type **21** in the main menu to open Menu 21.

```

Menu 21 - Filter Set Configuration

Filter                               Filter
Set #    Comments                    Set #    Comments
-----
 1      NetBIOS_WAN                    7      _____
 2      NetBIOS_LAN                    8      _____
 3      TEL_FTP_WEB_WAN                 9      _____
 4      _____                    10     _____
 5      _____                    11     _____
 6      _____                    12     _____

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Figure 8-3 Menu 21 – Filter Set Configuration

Step 2. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Step 3. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message “Press [ENTER] to confirm...” to open **Menu 21.1 – Filter Rules Summary**.

```

Menu 21.1 - Filter Rules Summary

# A Type                Filter Rules                M m n
-----
 1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137      N D N
 2 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138      N D N
 3 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139      N D N
 4 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137     N D N
 5 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138     N D N
 6 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139     N D F

Enter Filter Rule Number (1-6) to Configure: 1
    
```

Figure 8-4 Menu 21.1 – Filter Rules Summary

```

Menu 21.2 - Filter Rules Summary

# A Type                Filter Rules                M m n
-----
 1 Y IP  Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53  N D F
 2 Y
 3 Y
 4 Y
 5 Y
 6 Y

Enter Filter Rule Number (1-6) to Configure: 1
    
```

Figure 8-5 Menu 21.2 – Filter Rules Summary

8.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in Menus 21.1 and 21.2.

Table 8-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP, "IPX" for IPX.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

- For filter types IP, GEN (generic) and IPX the following rule abbreviations will be used.

Table 8-2 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number

GEN	
Off	Offset
Len	Length
IPX	
PT	IPX Packet Type
SS	Source Socket
DS	Destination Socket

8.3 Configuring a Filter Rule

To configure a filter rule, Type its number in **Menu 21.1 – Filter Rules Summary** and press [ENTER] to open Menu 21.1.1 for the rule.

There are three types of filter rules: **TCP/IP**, **IPX** and **Generic**. Depending on the type of rule, the parameters for each the type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

8.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, e.g., UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 – TCP/IP Filter Rule**, as shown next.


```

Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
               IP Mask= 0.0.0.0
               Port #= 137
               Port # Comp= Equal
Source: IP Addr= 0.0.0.0
         IP Mask= 0.0.0.0
         Port #= 0
         Port # Comp= None

TCP Estab= No
More= No      Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
    
```

Figure 8-6 Menu 21.1.1 – TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 8-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule coordinates, i.e., 2, 3 refers to the second filter set and the third filter rule of that set.	
Filter Type	Use [SPACE BAR] to toggle between types of rules. Parameters displayed for each type will be different.	TCP/IP Filter Rule/ Generic Filter Rule/ IPX Filter Rule
Active	This field activates/deactivates the filter rule.	Yes/No
IP Protocol	This is the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255.	0 to 255
IP Source Route	If Yes , the rule applies to packet with IP source route option; or else the packet must not have the source route option. The majority of IP packets do not have source route.	Yes/No
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr	IP mask

FIELD	DESCRIPTION	OPTIONS
	field.	
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port # .	None/Less/Greater/Equal/Not Equal
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the Source: IP Addr field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port # field.	None/Less/Greater/Equal/Not Equal
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If Yes , the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	Yes/No
More	If Yes , a matching packet is passed to the next filter rule before an action is taken; or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A.	Yes/No
Log	Select the logging option from the following: None – No packets will be logged. Action Matched – Only packets that match the rule parameters will be logged. Action Not Matched – Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a matching packet.	Check Next Rule/Forward/Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule/Forward/Drop
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

The following figure illustrates the logic flow of an IP filter.

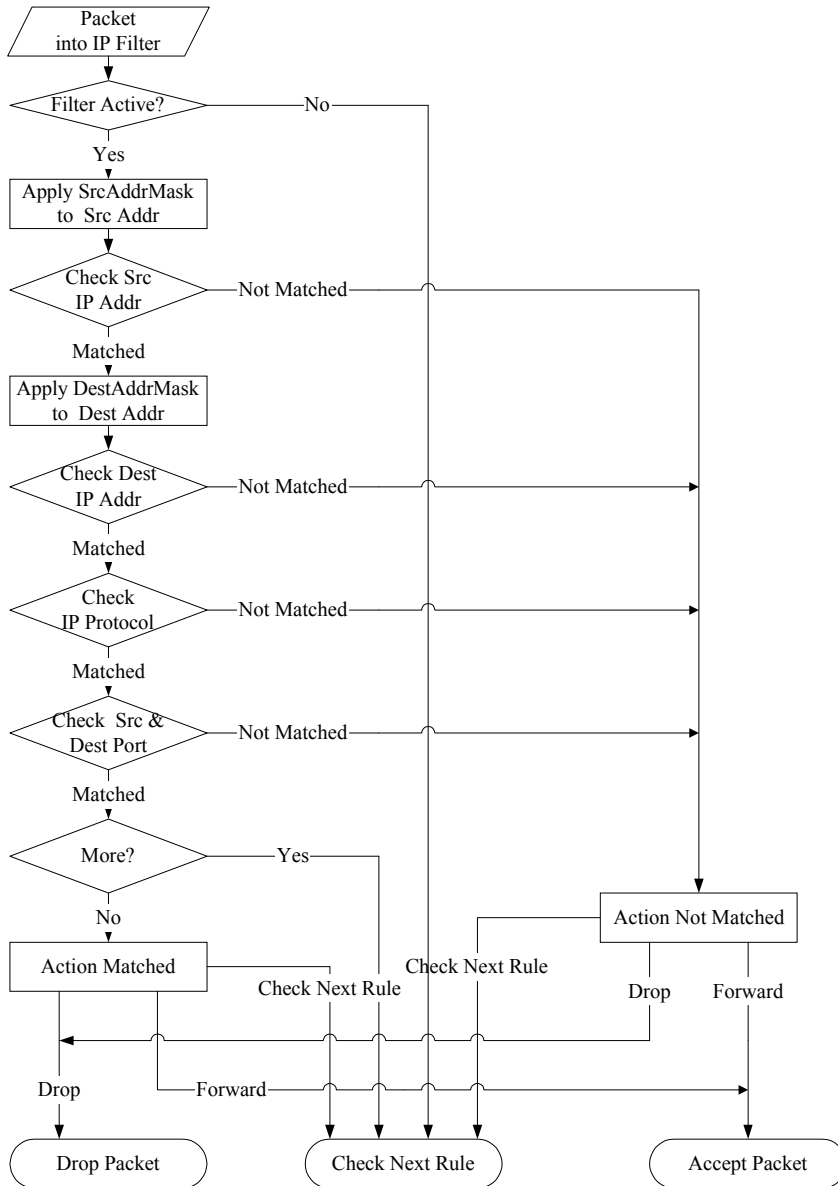


Figure 8-7 Executing an IP Filter

8.3.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the Offset (from 0) and the Length fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The Mask and Value are specified in hexadecimal numbers.

Two hexadecimal digits represent a byte, so if the length is 4, the value in either field will take 8 digits, e.g., FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for eg., 5. Select the **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.5.1 – Generic Filter Rule**, as shown in the following figure.

```
Menu 21.5.1 - Generic Filter Rule

Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 8-8 Menu 21.1.1 – Generic Filter Rule

The next table describes the fields in the Generic Filter Rule menu.

Table 8-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule coordinates, i.e., 2, 3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] to toggle between types of rules. Parameters displayed below each type will be different.	Generic Filter Rule/ TCP/IP Filter Rule/ IPX Filter Rule
Active	Select Yes to turn on the filter rule.	Yes/No
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If Yes , a matching packet is passed to the next filter rule before an action is taken; or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	Yes/No
Log	Select the logging option from the following: None – No packets will be logged. Action Matched – Only matching packets and rules will be logged. Action Not Matched – Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a matching packet.	Check Next Rule/Forward/ Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule/Forward/ Drop
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

8.3.3 Novell IPX Filter Rule

This section shows you how to configure an IPX filter rule. IPX filters allow you to base the rules on the fields in the IPX headers.

To configure an IPX rule, select **IPX Filter Rule** from the Filter Type field and press [ENTER] to open **Menu 21.1.1 – IPX Filter Rule**, as shown in the next figure.

```
Menu 21.1.1 - IPX Filter Rule

Filter #: 1,1
Filter Type= IPX Filter Rule
Active= No
IPX Packet Type=
Destination: Network #=
                Node #=
                Socket #=
                Socket # Comp= None
Source: Network #=
                Node #=
                Socket #=
                Socket # Comp= None
Operation= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 8-9 Menu 21.1.1 – IPX Filter Rule

The following table describes the IPX Filter Rule.

Table 8-5 IPX Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule coordinates, i.e., 2,3 refers to the second filter set and the third filter rule of that set.	e.g. 2,3
Filter Type	Use [SPACE BAR] to toggle between types of rules. Parameters displayed for each type will be different.	Device Filter Rule/ TCP/IP Filter Rule/ IPX Filter Rule
Active	Select Yes to turn on the filter rule.	Yes/No
IPX Packet Type	Type the IPX packet type (1-bit in hexadecimal) you want to filter. The more popular types are (in hexadecimal format): 01 – RIP 04 – SAP 05 – SPX (Sequenced Packet eXchange) 11 – NCP (NetWare Core Protocol) 14 – Novell NetBIOS	e.g. 14
Destination: Network #	Type the destination network numbers (4-byte in hexadecimal) of the packet that you want to filter.	e.g. 22222222
Node #	Type the destination node number (6-byte in hexadecimal) of the packet you want to filter.	e.g. 333333333333
Socket #	Type the destination socket number (2-byte in hexadecimal) of the packets that you want to filter.	e.g. 4444
Socket # Comp	Select the comparison you want to apply to the destination socket in the packet against that specified above.	None/Equal/ Not Equal/ Less/Greater
Source: Network #	Type the source network numbers (4-byte in hexadecimal) of the packet that you want to filter.	e.g. 55555555
Node #	Type the source node number (6-byte in hexadecimal) of the packet you want to filter.	e.g. 666666666666
Socket #	Type the source socket number (2-byte in hexadecimal) of the packets that you want to filter.	e.g. 7777
Socket # Comp	Select the comparison you want to apply to the source socket in the packet against that specified above.	None/Equal/ Not Equal/ Less/Greater

FIELD	DESCRIPTION	OPTIONS
Operation	This field applies only if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field to specify the type of the packet.	None/ RIP Request/ RIP Response/ SAP Request/ SAP Response/ SAP Get Nearest Server Request/ SAP Get Nearest Server Response.
More	If Yes , a matching packet is passed to the next filter rule before an action is taken; or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A.	Yes/No
Log	Select the logging option from the following: <ul style="list-style-type: none"> • None – No packets will be logged. • Action Matched – Only packets that match the rule parameters will be logged. • Action Not Matched – Only packets that do not match the rule parameters will be logged. • Both – All packets will be logged. 	None Action Matched Action Not Matched Both
Action Matched	Select the action for a matching packet.	Check Next Rule/Forward/ Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule/Forward/ Drop
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

8.4 Filter Types and SUA

There are two classes of filter rules, Device Filter rules and Protocol Filter (TCP/IP and IPX) rules. Device Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP and IPX packets.

When NAT/SUA (Network Address Translation/Single User Account) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the “native” IP address and port number before NAT/SUA for outgoing packets and after NAT/SUA for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; i.e., the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

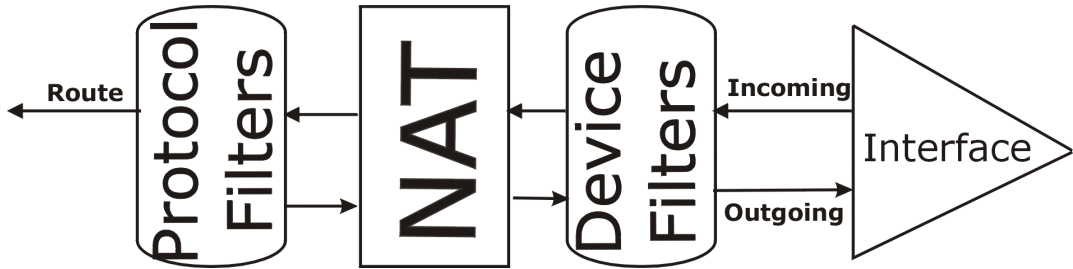


Figure 8-10 Protocol and Device Filter Sets

8.5 Filter Configuration Example

Let us look at part of the third default ZyXEL filter as an example. *See the Support CD* for more sample filters. This filter was designed to block outside users from telnetting into the Prestige.

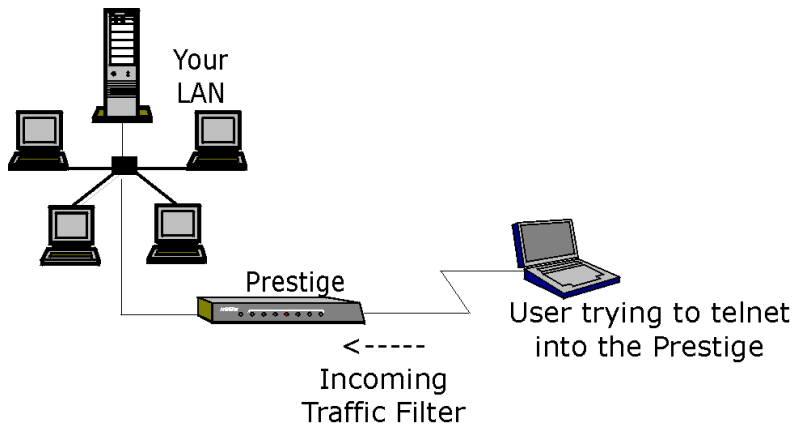


Figure 8-11 Sample Telnet Filter

- Step 1.** Type **21** from the main menu to open **Menu 21 – Filter Set Configuration**.
- Step 2.** Type the index of the filter set you want to configure (in this case 3) and press [ENTER].
- Step 3.** Type a descriptive name or comment in the **Edit Comments** field (for eg. TELNET_WAN) and press [ENTER].
- Step 4.** Press [ENTER] at the message “Press [ENTER] to confirm or [ESC] to cancel” to open **Menu 21.3 – Filter Rules Summary**.

```

Menu 21.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port # = 23
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port # =
        Port # Comp= None

TCP Estab= No
More= No           Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:
    
```

Press [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

6 is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See RFC-1060 for port numbers of well-known services.

Select **Equal** here as we are looking for packets going to port 23 only.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select **Next** if there are more rules to check.

There are no more rules to check.

Figure 8-12 Sample Filter – Menu 21.3.1

Step 5. Type **1** to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

```

Menu 21.3 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23  N D N
2 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21  N D N
3 Y IP Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80  N D F
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure: 1

```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched and there are no more rules in this set to be checked. **n=N** means there are more rules in this set to be checked.

Figure 8-13 Sample Filter Rules Summary – Menu 21.3

After you have created the filter set, you must apply it.

Step 1. Type **11** in the main menu to go to Menu 11 and type the remote node number to edit.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 3. This brings you to Menu 11.5. Apply the example filter set (eg. filter set 3) in this menu as shown in the next section.

8.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in Menu 21 (but have not been applied) to filter traffic.

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

8.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to Menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, e.g., 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in Menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

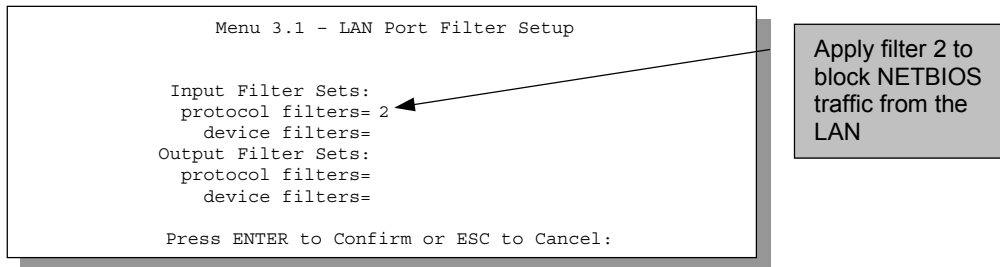


Figure 8-14 Filtering Ethernet Traffic

8.6.2 Remote Node Filters

Go to Menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in **protocol filters** field under **Call Filter Sets** in Menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

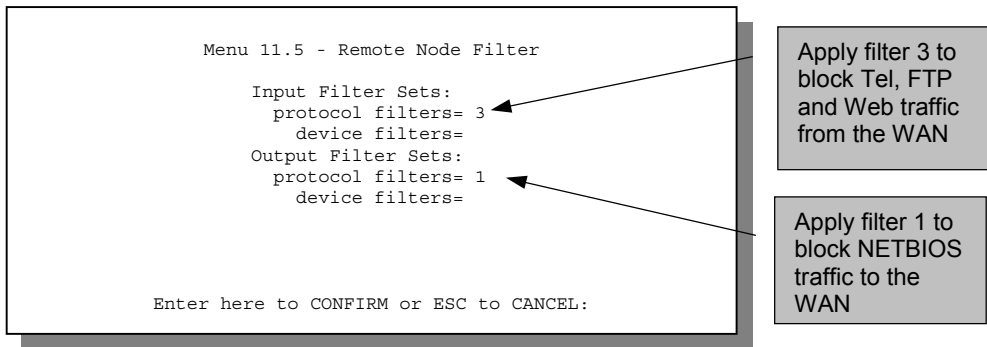


Figure 8-15 Filtering Remote Node Traffic

Chapter 9

SNMP Configuration

This chapter explains SNMP Configuration Menu 22.

SNMP is only available if TCP/IP is configured.

9.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

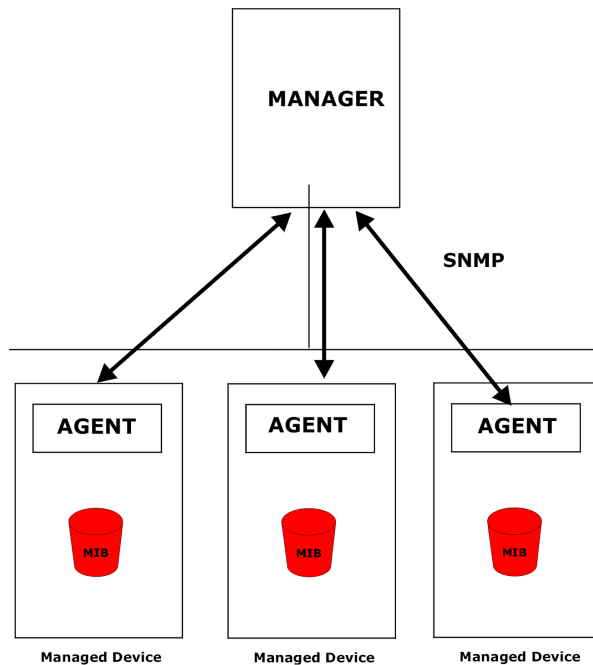


Figure 9-1 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

9.2 Supported MIBs

The Prestige supports MIB II that is defined in RFC-1213 and RFC-1215. The Prestige can also respond with specific data from the ZyXEL private MIB (ZYXEL-MIB). The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

The only implement MIBs in the Prestige as a SNMP agent. Users must implement their own GUI on SNMP platform (SNMP manager).

9.3 SNMP Configuration

To configure SNMP, select option **22** from the main menu to open **Menu 22 - SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.


```

Menu 22 - SNMP Configuration

SNMP:
Get Community= public
Set Community= public
Trusted Hgst= 0.0.0.0
Trap:
Community= public
Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

Figure 9-2 Menu 22 - SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 9-1 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	OPTIONS
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.	Public
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	Public
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.	Blank
Trap: Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	Public
Trap: Destination	Type the IP address of the station to send your SNMP traps to.	Blank

When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.

9.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 9-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent with the port number.
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
5	whyReboot (<i>defined in ZYXEL-MIB</i>)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warmstart).
5a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (e.g. download new files, CLI command "sys reboot", etc.).
5b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.
6	linkDown (<i>defined in RFC-1215</i>)	A trap is sent with the port number when any of the links are down. See the following table.

The port number is its interface index under the interface group.

Table 9-3 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
...	...
13	12
14	xDSL

Chapter 10

System Maintenance

This chapter covers the diagnostic tools that help you to maintain your Prestige.

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type **24** in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
10. Time and Date Setting

Enter Menu Selection Number:
```

Figure 10-1 Menu 24 – System Maintenance

10.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your G.SHDSL telephone line status, number of packets sent and received.

To get to System Status, type **24** to go to **Menu 24 – System Maintenance**. From this menu, type **1**. **System Status**. There are two commands in **Menu 24.1 – System Maintenance – Status**. Typing **1** resets the counters, [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status** which are READ-ONLY and meant for diagnostic purposes.

```

Menu 24.1 - System Maintenance - Status

Node-Lnk      Status  TxPkts  RxPkts  Errors  Tx B/s  Rx B/s  Up Time
1-ENET        Up      211     0       0       0       0       0:26:2
2             N/A    0       0       0       0       0       0:00:00
3             N/A    0       0       0       0       0       0:00:00
4             N/A    0       0       0       0       0       0:00:00
5             N/A    0       0       0       0       0       0:00:00
6             N/A    0       0       0       0       0       0:00:00
7             N/A    0       0       0       0       0       0:00:00
8             N/A    0       0       0       0       0       0:00:00
9             N/A    0       0       0       0       0       0:00:00
10            N/A    0       0       0       0       0       0:00:00
11            N/A    0       0       0       0       0       0:00:00
12            N/A    0       0       0       0       0       0:00:00

Ethernet:
Status: 10M/Half Duplex      Tx Pkts: 53
Collisions: 0                Rx Pkts: 36
CPU Load= 3.8%

WAN:
Line Status: Up
Transfer Rate: 2320 Kbps

Press Command:
COMMANDS: 1-Reset Counters  ESC-Exit
    
```

Figure 10-2 Menu 24.1 – System Maintenance – Status

The following table describes the fields present in **Menu 24.1 – System Maintenance – Status**.

Table 10-1 System Maintenance – Status Menu Fields

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPP, ENET, 1483.
Status	Shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
Ethernet	Shows statistics for the LAN.
Status	Shows the current status of the LAN.
Tx Pkts	The number of transmitted packets to the LAN.

FIELD	DESCRIPTION
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	Shows statistics for the WAN.
Line Status	Shows the current status of the xDSL line which can be Up or Down.
Transfer Rate	Shows the transfer rate based on Menu 2 – WAN Setup when the preceding field Line Status is Up.
CPU Load	Specifies the percentage of CPU utilization.

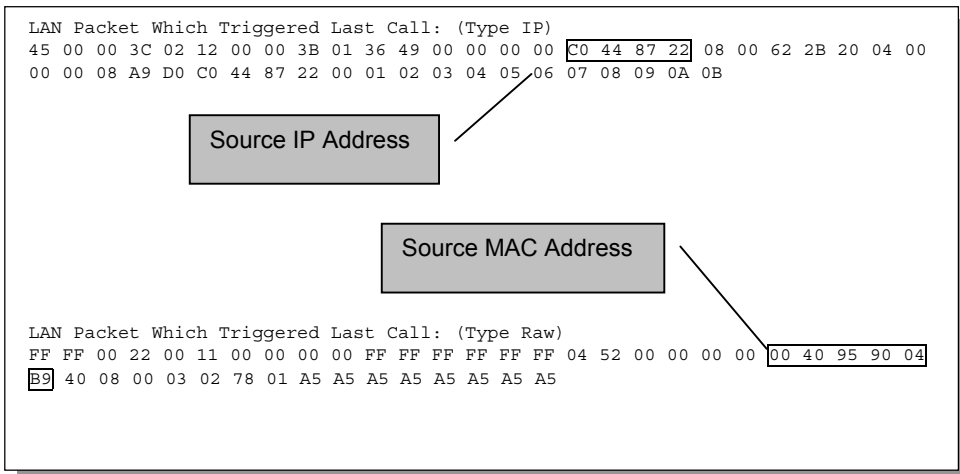


Figure 10-3 LAN Packet That Triggered Last Call

The figure above shows two samples of triggering packets from the LAN: the first of an ICMP ping packet (Type: IP) and the second a SAP broadcast packet (Type: Raw). With this information, you can determine the computer from the source IP address or the source MAC address of the packet.

10.1.1 System Information

```

Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V2.50(BH.0)b5 | 12/12/2000
xDSL F/W Version: A.102
Country Code: 255

LAN
Ethernet Address: 00:a0:c5:01:23:45
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
    
```

Figure 10-4 System Maintenance – Information

Table 10-2 Fields in System Maintenance

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of the ZyNOS Network Operating System firmware. ZyNOS is a registered trademark of ZyXEL Communications Corp.
xDSL F/W Version	Displays the G.SHDSL modem firmware version.
Country Code	Refers to the one byte country code value (in decimal notation).
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay, or Server) of the Prestige.

10.1.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200bps. Use [SPACE BAR] to select the desired speed in Menu 24.2.2, as shown in the following figure.

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 10-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed

10.2 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

10.2.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- Step 1.** Type **24** in the main menu to open **Menu 24 – System Maintenance**.
- Step 2.** From **Menu 24**, type **3** to open **Menu 24.3 – System Maintenance – Log and Trace**.
- Step 3.** Type **1** from **Menu 24.3 – System Maintenance – Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
60      4 PP07  INFO  LAN promiscuous mode <0>
61      4 PINI  ERROR System Ert completed
63      e PINI  INFO  Session Begin
Clear Error Log (y/n):
```

Figure 10-6 Sample Error and Information Messages

10.2.2 Syslog and Accounting

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 – System Maintenance – UNIX Syslog**, as shown next.

```

Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
  Active= No
  Syslog IP Address= ?
  Log Facility= Local 1

Types:
  CDR= No
  Packet triggered= N/A
  Filter Log= No
  PPP Log= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
    
```

Figure 10-7 Menu 24.3.2 – System Maintenance – Syslog and Accounting

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 10-3 System Maintenance Menu – Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] to turn on or off syslog.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] to toggle between the 7 different Local options. The log facility lets you to log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to Yes .
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to Yes .
Filter Log	No filters are logged when this field is set to No. Filters with the individual filter Log Filter field set to Yes are logged when this field is set to Yes .
PPP Log	PPP events are logged when this field is set to Yes .

The following are examples of the four types of syslog messages sent by the Prestige:

1 - CDR
SdcmSyslogSend (SYSLOG CDR, SYSLOG INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1, C02 Call Terminated

2 - Packet Triggered
SdcmSyslogSend (SYSLOG PKTRRI, SYSLOG NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxxxxx...x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log
SdcmSyslogSend (SYSLOG FILLOG, SYSLOG NOTICE, String);
String = IP[Src=xx.xx.xx Dst=xx.xx.xx prot =xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m), drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZyXEL Communications Corp.: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZyXEL Communications Corp.: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZyXEL Communications Corp.: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF

4 - PPP Log			
SdcmdSyslogSend (SYSLOG PPLOG, SYSLOG NOTICE, String);			
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown			
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP			
Jul 19 11:42:44	192.168.102.2	ZyXEL Communications Corp.:	ppp:LCP Closing
Jul 19 11:42:49	192.168.102.2	ZyXEL Communications Corp.:	ppp:IPCP Closing
Jul 19 11:42:54	192.168.102.2	ZyXEL Communications Corp.:	ppp:CCP Closing

10.3 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

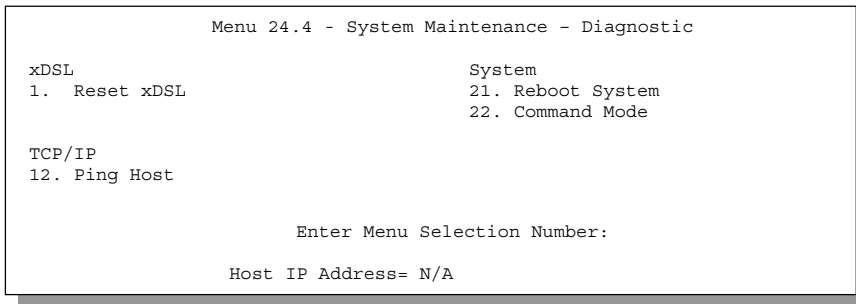


Figure 10-8 Menu 24.4 – System Maintenance – Diagnostic

Follow the procedure next to get to Diagnostic:

- Step 1.** From the main menu, type **24** to open **Menu 24 – System Maintenance**.
- Step 2.** From this menu, type **4**. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

The following table describes the diagnostic tests available in Menu 24.4 for and the connections.

Table 10-4 System Maintenance Menu – Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

10.4 Filename Conventions

The configuration file (sometimes called the romfile or rom-0) contains the settings in the menus such as password, DHCP Setup defaults, TCP/IP Setup defaults, etc. The external (i.e., not on the Prestige) configuration filename is usually the router model name with a *.rom extension. The ZyNOS firmware file (sometimes called the “ras” file) contains the ZyXEL Network Operating System firmware and the external firmware file is usually the router model name with a *.bin extension. Rename the configuration filename to “rom-0” and the firmware filename to “ras” when transferring files to the Prestige (i.e., the internal filenames on the Prestige). Renaming the files is not necessary when you transfer files using the Xmodem protocol.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, i.e., on your computer, local network, or ftp site and so the name (but not the extension) will vary. Type the AT command after you press **Y** when prompted in the SMT menu to go into debug mode. After uploading the new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1** to check if you uploaded the correct firmware version.

Table 10-5 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION	AT COMMAND
Configuration File	Rom-0	*.rom	This is the Prestige router configuration filename. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (also the speed and default password), the error and trace logs.	ATLC
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.	ATUR

10.5 Backup Configuration

Typing **5** in **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly.

You must perform backup and restore through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload.

Note that the terms “download” and “upload” are relative to the computer. Download means to transfer from another computer to the workstation, while upload means from your computer to another computer.

Step 1. Go to Menu 24.5 (shown next).

```
Ready to backup Configuration via Xmodem.  
Do you want to continue (y/n):
```

Figure 10-9 Backup Configuration

Step 2. Press **Y** to indicate that you want to continue.

The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar. Run the HyperTerminal program.

Step 1. Click “Transfer”, then “Receive File” to display the following screen.

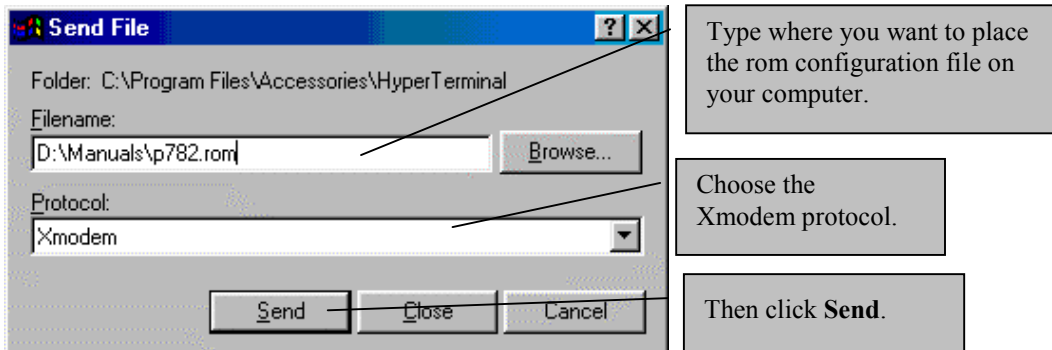


Figure 10-10 HyperTerminal Screen

Step 2. Type a path and name for the rom configuration file on your computer and make sure you choose the Xmodem protocol. Then press “Receive”.

Step 3. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

```
** Backup Configuration completed. OK.  
### Hit any key to continue.###
```

Figure 10-11 Successful Backup

10.6 Restore Configuration

Type **6** in **Menu 24 – System Maintenance** to restore the configuration from your computer to the Prestige. Again, you must use the console port and Xmodem protocol to restore the configuration.

Keep in mind that the configuration is stored in the flash ROM in the Prestige, so even if power failure should occur, your configuration is safe.

Step 1. Go to Menu 24.6 (shown next).

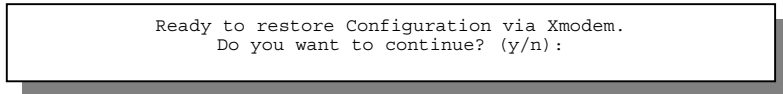


Figure 10-12 Restore Configuration

Step 2. Press **Y** to continue.

The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar. Run the HyperTerminal program.

Step 3. Click **Transfer**, then **Send File** to display the following screen.

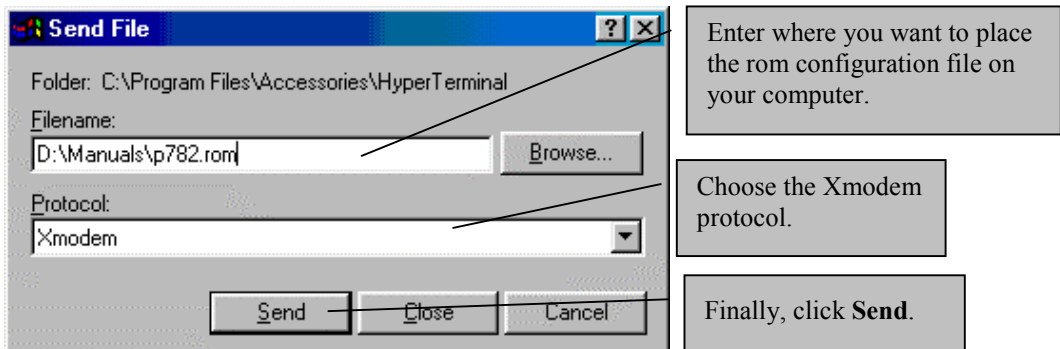


Figure 10-13 HyperTerminal Screen

Step 4. Type the location on your computer of the rom configuration file and make sure you choose the Xmodem protocol. Then press **Send**.

Step 5. After a successful restoration you will see the following screen. Press any key to return to reboot the system.

```
Save to ROM
Hit any key to start system reboot.
```

Figure 10-14 Successful Restoration

Keep in mind that the configuration is stored in the flash ROM in the Prestige, so even if power failure should occur, your configuration is safe.

10.7 Upload Firmware

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file via the console port. The firmware and configuration file may also be uploaded via FTP. There are 2 components in the system: the router firmware and the configuration file, as shown in the next figure. Restoring the configuration as in Menu 24.6 copies your (customized) backup configuration from your computer to the Prestige. Note that you must be able to access the SMT to do this. Uploading the configuration file via Menu 24.7.2 on the other hand rewrites all configuration data, as well as system-related data, the error log and the trace log. If you forget your password for instance you will need to use Menu 24.7.2 as you can use this method in debug mode. However, your customized settings will be reset to the default values (including your password being reset to 1234, the Prestige default password).

```
Menu 24.7 - System Maintenance - Upload Firmware

1. Upload System Firmware
2. Upload System Configuration File

Enter Menu Selection Number:
```

Figure 10-15 Menu 24.7 – System Maintenance – Upload Firmware

10.7.1 Upload Router Firmware

The firmware is the program that controls the functions of the Prestige. **Menu 24.7.1** shows you the instructions for uploading the firmware. If you type **Y** at the prompt, the Prestige will go into debug mode. Follow the procedure next to upload the firmware:

- Step 1.** Type **atur** after the “Enter Debug Mode” message.
- Step 2.** Wait for the **Starting Xmodem upload** message before activating **Xmodem** upload on your terminal.
- Step 3.** After successful firmware upload, type **atgo** to restart the Prestige.

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload system firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   XMODEM upload on your terminal.
4. After successful firmware upload, type "atgo" to restart the
   system.

Warning: Proceeding with the upload will erase the current system
firmware.

Do You Wish To Proceed? (Y/N)
```

Figure 10-16 Menu 24.7.1 – Uploading Router Firmware

10.7.2 Uploading Router Configuration File

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

Menu 24.7.2 shows you the instructions for uploading the configuration file. If you type **Y** at the prompt, the Prestige will go into debug mode. Follow the next procedure to upload the configuration file:

Step 1. Type **atlc** after the **Enter Debug Mode** message.

Step 2. Wait for the **Starting Xmodem upload** message before activating **Xmodem** upload on your terminal.

Step 3. After successful configuration file upload, type **atgo** to restart the Prestige.

If you replace the current configuration file with the default configuration file, you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity, 1 stop bit (8n1) and no Flow Control. You will need to change your serial communications software to the default before you can reconnect to the Prestige. The password will be reset to the default of 1234.

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   XMODEM upload on your terminal.
4. After successful firmware upload, type "atgo" to restart the
   system.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The system's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (Menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".

Do You Wish To Proceed? (Y/N)
```

Figure 10-17 Menu 24.7.2 – System Maintenance – Upload Router Configuration File

10.7.3 TFTP Transfer

In addition to the direct console port connection, the Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Even though TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the next procedures:

- Step 1.** Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security check, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Place the SMT in command interpreter (CI) mode by typing **8** in **Menu 24 – System Maintenance**.
- Step 3.** Type command **sys stdio 0** to disable SMT timeout, so the TFTP transfer will not be interrupted.
- Step 4.** Launch TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

- Step 5.** Use the TFTP client to transfer files between the Prestige and the computer. The firmware file name is **ras** and for the configuration file, **rom-0** (rom-zero, not capital o).

If you upload the firmware to the Prestige, it will reboot automatically when the file transfer is completed.

The Telnet connection must be active and the SMT in CI mode before and during the TFTP transfer.

For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use **get** to transfer from the Prestige to the computer, **put** the other way around and **binary** to set binary transfer mode.

With serial (Xmodem) transfer, the filenames on the PC are your choice. With many ftp and tftp clients, they are as well as seen next.

ftp> put **prestige.bin ras**

This is a sample ftp session showing the transfer of the PC file **prestige.bin** to the Prestige.

ftp> get rom-0 **prestige.cfg**

This is a sample ftp session saving the current configuration to the PC file **prestige.cfg**.

Using the FTP Command from the DOS Prompt

Step 1. Launch the FTP client on your computer.

Step 1. Type **open** and the IP address of your Prestige.

Step 2. You may press [ENTER] when prompted for a username.

Step 3. Type **root** and your SMT password as requested. The default is 1234.

Step 4. Type **bin** to set transfer mode to binary.

Step 5. Use **put** to transfer files from the computer to the Prestige, e.g., **put prestige.bin ras** transfers the firmware on your computer (prestige.bin) to the Prestige and renames it **ras**. Similarly **put prestige.rom rom** transfers the configuration file on your computer (prestige.rom) to the Prestige and renames it **rom**.

Step 6. Type **quit** to exit the ftp prompt.

```

Connected to 782.x.x.x
220 prestige FTP version 1.0 ready at Thu Jan  8 18:00:02 2001
User (782.x.x.x:(none)): <Enter>
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put prestige.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
    
```

Figure 10-18 Sample FTP Session

The following table describes some of the fields that you may see in third-party FTP clients.

Table 10-6 Third Party FTP Clients – General Fields

FIELD	DESCRIPTION	OPTIONS
Host Address	Type the address of the host server	Parameters for the Prestige
Login Type	<p>Anonymous</p> <p>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.</p> <p>Normal</p> <p>The server requires a unique User ID and Password to login.</p>	Normal
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.	Binary
Initial Remote Directory	Specify the default remote directory (path).	
Initial Local Directory	Specify the default local directory (path).	

The following table describes some of the fields that you may see in third-party TFTP clients.

COMMAND	DESCRIPTION
Host	Type your IP address. 192.168.1.1 is the Prestige default IP address when shipped.
Send/Fetch	Press [Send] to upload the file to the Prestige and [Fetch] to back up the file on your computer.
Local File	Type the path and firmware file name (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	The Prestige filename. The firmware filename is ras . The configuration file, is rom-0 .
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

10.7.4 Boot Module Commands

When you reboot your Prestige, you will be given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example **ATUR** (for uploading firmware) and **ATLC** (for uploading the configuration file) already discussed in a previous section.

```

Bootbase Version: V2.00 | 4/14/2001 13:58:03
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2

ZyNOS Version: V2.50(BH.0)b5 | 12/12/2001 14:01:55

Press any key to enter debug mode within 3 seconds.
.....

```

Figure 10-19 Option to Enter Debug Mode

Type **ATHE** to view all available Prestige boot module commands. Some are shown in the next screen. Most commands aid in advanced troubleshooting and should only be used by qualified engineers.

```
          ===== Debug Command Listing =====
ATHE      print help
ATGO      boot system
ATUR      upload RAS code
ATLC      upload RAS configuration file
ATBAX     change baud rate. 1:38.4, 2:19.2, 3:9.6, 4:57.6,
ATTD      5:115.2
ATSE      download configuration to PC
ATSH      display seed for password generation
           display Revision, etc.
```

Figure 10-20 Boot Module Commands

10.8 Command Interpreter Mode

This option allows you to enter the command interpreter mode. A list of valid commands can be found by typing [help] at the command prompt. For more detailed information, check the ZyXEL web site or send e-mail to the ZyXEL Support Group.

```
          Enter Menu Selection Number: 8

Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          wan
xdsl        atm           ip            bridge
ipx
ras>
```

Figure 10-21 Command Mode

10.9 Time and Date Setting

This feature allows the Prestige to connect to a timeserver to synchronize its system clock when it is booting. There is no Real Time Chip (RTC) chip in the Prestige, so this software mechanism allows you to get the current time and date from an external server when you power up your Prestige. Go to **Menu 24.10** to update the time and date settings of your Prestige.

```

Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server IP Address= N/A

Current Time:                00 : 00 : 00
New Time (hh:mm:ss):        04 : 16 : 42

Current Date:                2001 - 01 - 01
New Date (mm-dd-yyyy):      2001 -01 - 01

Time Zone= GMT

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
    
```

Figure 10-22 System Maintenance – Time and Date Setting

Table 10-7 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server at Bootup=	Type the time service protocol that your timeserver sends at bootup. Option are Daytime (RFC 867) , Time (RFC-868) , NTP (RFC-1305) and None . The formats differ, e.g., the Daytime (RFC 867) format is day/month/date/year/time zone of the server while the Time (RFC-868) format gives a 4-byte integer giving the total number of seconds since 1/1/1970 at 0:0:0. The NTP (RFC-1305) format is similar. Not all timeservers support all protocols, so check with your ISP/network administrator or use trial and error to find a viable protocol. If you select None (the default value) you can change the time manually, but at each reboot the time & date will reset to 2000-01-01 0:0:0 .
Time Server IP Address=	Type the IP address of the your timeserver. Check with your ISP/network administrator if you are unsure of this information.
Current Time: New Time	Type the current time. Type the new time in hour, minute and second format.
Current Date: New Date	Type the current date. Type the new date in year, month and date format.
Time Zone= GMT+	Press [SPACE BAR] to set: Greenwich Mean Time (GMT) plus number of hours to your time zone. Note: Daylight savings time alters this time.
On completion, press [ENTER] to save the setting and press [ESC] to return to Menu 24 .	

Chapter 11

IP Routing Policy

This chapter covers IP routing policy.

11.1 Introduction

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

11.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

11.3 Routing Policy

A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

11.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

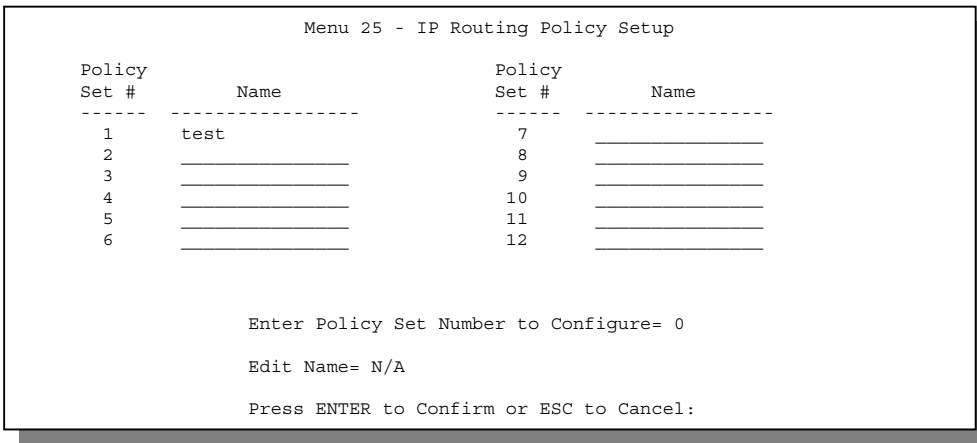


Figure 11-1 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

- Step 1.** Type **25** in the main menu to open **Menu 25 – IP Routing Policy Setup**.
- Step 2.** Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “[” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.


```

Menu 25.1 - IP Routing Policy Setup

# A                               Criteria/Action
- - - - -
1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
   SP=20-25,DP=20-25,P=6,T=NM,PR=0      |GW=192.168.1.1,T=MT,PR=0
2 N _____
3 N _____
4 N _____
5 N _____
6 N _____

Enter Policy Rule Number (1-6) to Configure:
    
```

Figure 11-2 Menu 25.1 – Sample IP Routing Policy Setup

Table 11-1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17...)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

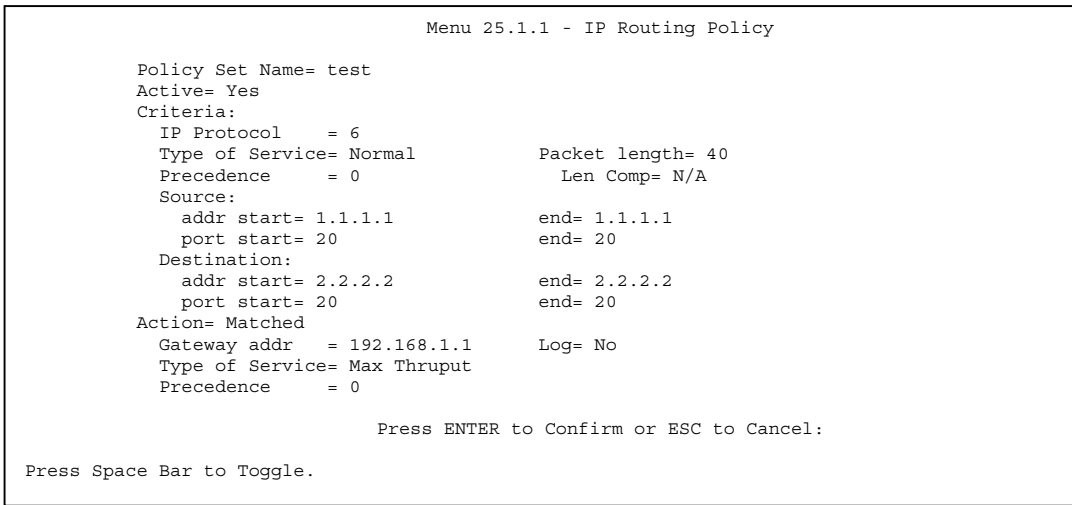


Figure 11-3 IP Routing Policy

Table 11-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in Menu 25 – IP Routing Policy Setup .
Active	Press [SPACE BAR] to select Yes to activate the policy.
Criteria	
IP Protocol	IP layer 4 protocol, e.g., UDP, TCP, ICMP , etc.
Type of Service	Prioritize incoming network traffic by choosing from Don't Care / Normal / Min Delay / Max Thruput / Max Reliability .
Precedence	Precedence value of the incoming packet. Values are 0 to 7 or Don't Care .
Packet Length	Type the length of incoming packets (in bytes). The operators in the Len Comp (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] to choose from Equal / Not Equal / Less / Greater / Less or Equal / Greater or Equal .
Source:	

FIELD	DESCRIPTION
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched .
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Choose from prioritize incoming network traffic by choosing from No Change / Normal / Min Delay / Max Thruput / Max Reliability / Min Cost .
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or No Change .
Log	Press [SPACE BAR] to select Yes to make an entry in the system log when a policy is executed.

11.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

11.5.1 Ethernet IP Policies

From **Menu 3 – Ethernet Setup**, type **2** to go to **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, e.g., 2, 4, 7, 9.

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup:
DHCP= None
Client IP Pool Starting Address= N/A
Size of Client IP Pool= N/A
Primary DNS Server= N/A
Secondary DNS Server= N/A
Remote DHCP Server= N/A

TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies= 2,4,7,9
Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:
```

Type IP Policy sets here.

Figure 11-4 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

Go to **Menu 11.3** (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:
Rem IP Addr: 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
Single User Account= No

Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies= 1,2,3,4

IPX Options:
Rem LAN Net #= N/A
My WAN Net #= N/A
Hop Count= N/A
Tick Count= N/A

Bridge Options:
Ethernet Addr Timeout (min)= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Type IP Policy sets here.

Figure 11-5 Menu 11.3 – Remote Node Network Layer Options

11.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

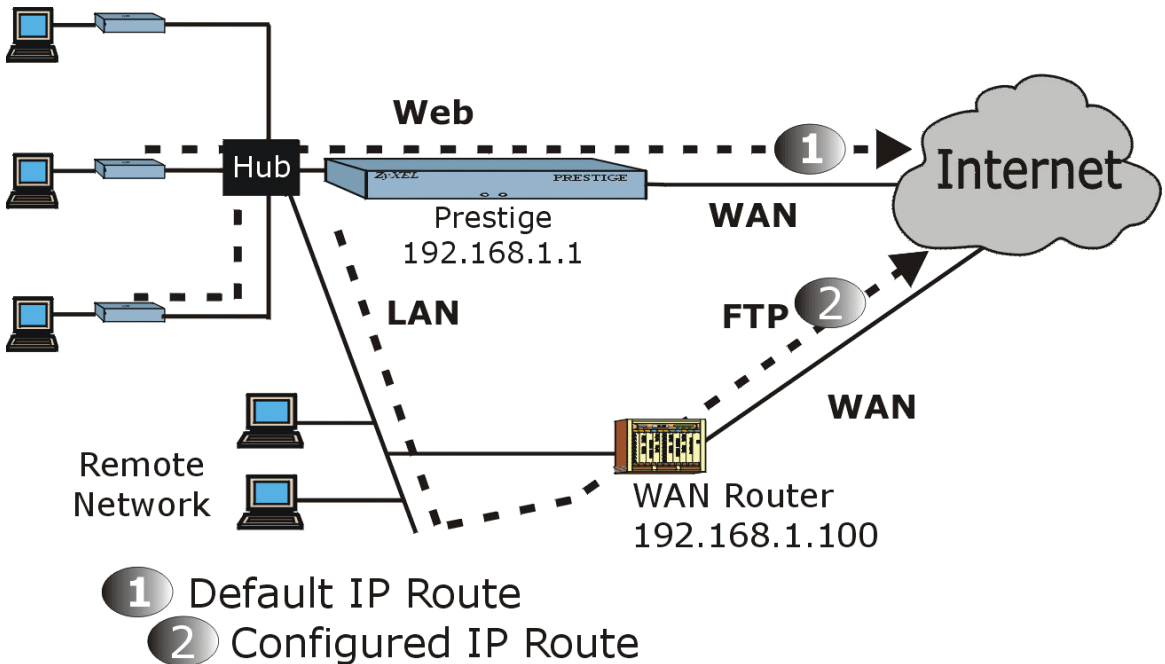


Figure 11-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

Step 1. Create a routing policy set in Menu 25.

Step 2. Create a rule for this set in **Menu 25.1 - IP Routing Policy** as shown next.

```
Menu 25.1 - IP Routing Policy

Policy Set Name= set1
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care
  Precedence      = Don't Care
  Packet length= 10
  Len Comp= N/A
Source:
  addr start= 192.168.1.2
  port start= 0
  end= 192.168.1.64
  end= N/A
Destination:
  addr start= 0.0.0.0
  port start= 80
  end= N/A
  end= 80
Action= Matched
Gateway addr  = 192.168.1.1
Type of Service= No Change
Precedence    = No Change
Log= No

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figure 11-7 IP Routing Policy Example

Step 3. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in **Menu 25**.

Step 5. Create a rule in **Menu 25.2** for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```

Menu 25.2 - IP Routing Policy

Policy Set Name= set2
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service = Don't Care
  Precedence      = Don't Care
  Packet length= 10
  Len Comp= N/A
Source:
  addr start= 0.0.0.0
  port start= 0
  end= N/A
  end= N/A
Destination:
  addr start= 0.0.0.0
  port start= 20
  end= N/A
  end= 21
Action= Matched
Gateway addr =192.168.1.100
Type of Service= No Change
Precedence = No Change
Log= No

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

Figure 11-8 IP Policy Routing

Step 6. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in **Menu 3.2** as shown next.

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 64
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup.
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-1
  Multicast= None
  IP Policies= 1,2
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 11-9 Applying IP Policies

Part: IV

ADDITIONAL INFORMATION

Part IV contains Troubleshooting, Power Adapter Specifications, a Glossary and the Index.

Chapter 12

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Table 12-1 Problems Starting the Prestige

PROBLEM	CORRECTIVE ACTION
No LEDs are on when the Prestige is turned on.	Check the connection between the adapter and the Prestige. If error persists, it may be a hardware problem. Contact technical support.
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's serial port.
	2. Check to see if the communications program is configured correctly. It should be configured as follows:
	VT100 terminal emulation. 9600 bps is the Prestige factory default speed. Try other speeds in case it has been changed. No parity, 8 Data bits, 1 Stop bit, No Flow Control.

Table 12-2 Problems connecting with the WAN or Remote Node/ISP

PROBLEM	CORRECTIVE ACTION
Cannot initialize the PVC connection.	Verify the xDSL port/wall jack cable connection. The xDSL LED should be on. If not, verify in Menu 24.1 that the Line Status is Down. Wait 10 minutes until the PVC synchronizes and the field reads Up. If the field does not eventually read Up, verify in Menu 2 that Service Type (Client or Server) and Transfer Rate are the same as the peer. If problems persist, check with the telephone company, ISP and/or the peer router (in a LAN-to-LAN application).
Cannot connect to a remote node or ISP.	Check Menu 4 or Menu 11.1 to verify the Encapsulation for the remote node.

Table 12-3 Problems connecting with the LAN

PROBLEM	CORRECTIVE ACTION
Cannot ping any station on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your Prestige and the station.
	Verify that the Prestige and workstations share the same IP address and subnet mask.

Appendix A

Power Adapter Specifications

SPECIFICATIONS	NORTH AMERICA	EUROPEAN UNION	UK
Part Number	30-112-120602	30-123-120601	30-123-120101
AC Power Adapter model	AD48-1201200DUY	AD-1201200DV	AD-1201200DK
Input power	AC120Volts/60Hz	AC230Volts/50Hz,	AC230Volts/50Hz,
Output power	DC12Volts/1.2A	DC12Volts/1.2A	DC12Volts/1.2A
Power consumption	7.5 W	7.5 W	7.5 W
Plug Standards	North American	European Union	United Kingdom
Safety standards	UL, CUL (UL1950, CSA C22.2 NO. 234- M90)	TUV, CE (EN 60950)	TUV, CE (EN 60950, BS7002)

Diagram 1 Power Adapter Specifications

Glossary

10BaseT	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5); one pair for transmitting data and the other for receiving data.
Analog	An electrical circuit that is represented by means of continuous, variable physical quantities (such as voltages and frequencies), as opposed to discrete representations (like the 0/1, off/on representation of digital circuits).
ARP	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
AT&T 5ESS	A digital central office switching system made by AT&T.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
Bit	A Binary Digit (either a one or a zero). A single digit number in base-2. A bit is the smallest unit of computerized data.
Boot Module Commands	Boot Module Commands, available in the debug mode via SMT, help you initialize the configuration of the basic functions and features of your Prestige such as uploading firmware, changing the console port speed and viewing product-related information.
Bridging	Bridging provides LAN to LAN frame forwarding services between two or more LANs. Frames from one LAN are forwarded across a bridge to a connected LAN, although filtering can be employed to selectively forward frames. Bridging works similar to the way repeaters work except that bridges forward frames based on their MAC (Medium Access Control) addresses which are hardware-level addresses of NICs (Network Interface Cards).
Byte	A set of bits that represent a single character. There are 8 bits in a Byte.
CDR	Call Detail Record. This is a name used by telephone companies for call-related information.
CHAP	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
Client	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or

	more specific kinds of Server programs and each Server requires a specific kind of Client. A Web Browser, for example, is a specific kind of Client.
CO	Central Office. A CO is a facility that serves local telephone subscribers. In the CO, subscribers' lines are joined to switching equipment that allows them to connect to each other for both local and long distance calls.
COE	Central Office Equipment. A central office is where home and office phone lines terminate and connect to a much larger switching system.
CPE	Customer Premise Equipment is privately-owned telecommunication equipment at an organization's site that is attached to the telecommunication network. CPE equipment includes routers, modems, PBXs, telephones, key systems, facsimile products, voice processing equipment and video communication equipment.
Crossover Ethernet Cable	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
Crosstalk	Crosstalk is noise emanating from the signals transmitted on adjacent wire pairs. Crosstalk is caused by electric or magnetic fields of one telecommunication signal affecting the signal in an adjacent circuit. In a telephone circuit, crosstalk can result in you hearing part of a voice conversation from another circuit. The phenomenon that causes crosstalk is called Electro Magnetic Interference (EMI). It can occur in microcircuits within computers and audio equipment as well as within network circuits.
CSU/DSU	Channel Service Unit/Data Service Unit. CSUs and DSUs are actually two separate devices, but they are used in conjunction and often combined into the same box. These devices are part of the hardware you need to connect computer equipment to digital transmission lines. The CSU device connects with the digital communication line and provides a termination for the digital signal. The DSU device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. This device converts signals from bridges, routers and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.
DCE	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
Device Filters	Your Prestige uses Device Filters to decide whether or not to allow passage of a data packet and/or to make a call. Device filters act on raw data from/to LAN and WAN, serve as a limited firewall to your Prestige and may be configured as Device Filter Rules via the SMT.
DHCP	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses for a period of time which

	means that addresses are made available to assign to other systems.
Digital	The use of a binary code to represent information, such as 0/1, or on/off.
DNS	Domain Name System. A database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.
Domain Name	The unique name that identifies an Internet site. Domain Names always have 2 or more parts that are separated by dots. Generally speaking, the part on the left is the most specific and the part on the right is the most general.
DRAM	Dynamic RAM stores information in capacitors that must be refreshed periodically.
DSL	Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions) or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits which means that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier's frame relay, ATM (Asynchronous Transfer Mode) or Internet-connect system.
DSLAM	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay or IP networks.
DTE	Originally, Data Terminal Equipment meant Dumb Terminal Equipment. But today it is a computer, bridge or router that interconnects local area networks (LANs) in increasingly more intelligent ways.
EMI	Electromagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
FAQ	Frequently Asked Questions. FAQs are documents that list and answer the most common questions on a particular subject.
FCC	The Federal Communications Commission is responsible for allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Flash Memory	Nonvolatile storage that can be electrically erased and reprogrammed so that data can

	be stored, booted and rewritten as necessary.
Frame Type	Each frame type is a separate logical network, even though they exist on one physical network. Frame Types are 802.2, 802.3, Ethernet II (DIX) and SNAP (Sub-Network Access Protocol).
FTP	File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. FTP is basically a client/server protocol in which a system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems.
G.SHDSL	A Single-pair High-speed Digital Subscriber Line is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire. The "G." in "G.SHDSL" is defined by the G.991.2 ITU (International Telecommunication Union) state-of-the-art industry standard. G.SHDSL provides data rates up to 2.3 Mbits/sec. Unlike traditional HDSL systems, which use two twisted pair, G.SHDSL reduces equipment and lease-line costs by providing the same service using only one twisted pair. See also DSL.
Gateway	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages and/or architecture.
HDLC	High-level Data Link Control is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host computer provide several services, such as WWW and USENET.
HTTP	Hyper Text Transfer Protocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.
IANA	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers and more.
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
Inside Wiring	Wiring that is done from the point of demarcation to the jack in the wall where the line terminates.
Internet	(Lower case i) Any time you connect 2 or more networks together, you have an

	internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
IP	Internet Protocol. The IP (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
IP Alias	Internet Protocol Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.
IP Pool	Internet Protocol Pool refers to the collective group of IP addresses located in any particular place (for example, LAN, WAN, Ethernet, etc.).
IP Routing Policy	Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Routing Policy (IPRP) provides a mechanism to override the default routing behavior and forward the packet based on the policy defined by the network administrator.
IPCP (PPP)	IP Control Protocol allows changes to IP parameters such as the IP address.
IPX	Internetwork Packet eXchange. Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services. The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange).
IRC	Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to "chat" over the network. Today IRC is a very popular way to "talk" in real time with other people on the Internet. However, IRC is also one avenue hackers use to obtain information about your system and/or company. Moreover, IRC sessions are prone to numerous attacks that, while not dangerous, can cause system crashes.
ISP	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
Jack Type	Different types of jacks (RJ11, RJ45 or RJ48) can be used for an ISDN line. The RJ11 is the most common in the world and is most often used for analog phones, modems and fax machines. RJ48 and RJ45 are essentially the same, as they both have the same 8-pin configuration. An RJ11 jack can fit into an RJ45/RJ48 connector, however, an RJ45/RJ48 cannot fit into an RJ11 connector.
LAN	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs

	were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.
LATA	Local Access and Transport Area is a geographic territory used primarily by local telephone companies to determine charges for intrastate calls. As a result of the Bell divestiture, switched calls that both begin and end at points within the LATA (intraLATA) are generally the sole responsibility of the local telephone company. Conversely, calls that cross outside the LATA (interLATA) are passed on to an Inter eXchange Carrier (IXC).
LEC	Local Exchange Carrier. The local phone companies – either a Regional Bell Operating Company (RBOC) or an independent phone company (e.g., GTE) – that provide local transmission services.
LED	Light Emitting Diode. LEDs are visual indicators that relay information about the status of specific Prestige functions to the user by lighting up, turning off or blinking. LEDs are usually found on the front panel of the physical device. Examples include Status, Power and System LEDs.
Linux	A version of the UNIX operating system designed to run on IBM Compatible computers.
LLC-Multiplexing	One VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, eg., if charging heavily depends on the number simultaneous VCs.
Loop-reach	Loop reach defines speed that can be attained at various distances. This is very important for DSL technology as distance from the CO (Central Office) influences attainable speeds.
MAC	On a local area network (LAN) or other network, the Media Access Control (MAC) address is your computer's unique hardware number. (On an Ethernet LAN, it is the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
Name Resolution	The allocation of an IP address to a host name. See also DNS.
NAT	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network. See also SUA.
NDIS	Network Driver Interface Specification is a Windows® specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.

NetBIOS	Network Basic Input/Output System. NetBIOS is an extension of the DOS BIOS that enables a computer to connect to and communicate with a LAN.
Network	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
Node	Any single computer connected to a network.
Packet Filter	A filter that scans packets and decides whether to let them through or not.
PAP	Password Authentication Protocol (PAP) is a security protocol that requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
Ping Attack	An attack that slows down the network until it is unusable. The attacker sends a "ping" command to the network repeatedly to slow it down. See also Denial of Service.
Point of Demarcation	The physical point where the phone company ends its responsibility with the wiring of the phone line.
POP	A Point of Presence is the point where long-distance telephone service providers connect into regional and local telephone systems.
POP	Post Office Protocol. This is a common protocol used for sending, receiving and delivering mail messages.
Port	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g., Web servers normally listen on port 80.
Port (H/W)	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.
POTS	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
PPP	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering

	Task Force) RFC-1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.
Promiscuous Packet Capture	Actively capturing packet information from a network. Most computers only collect packets specifically addressed to them. Promiscuous packet capture acquires all network traffic it can regardless of where the packets are addressed.
Protocol	A “language” for communicating on a network. Protocols are sets of standards or rules used to define, format and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
Protocol Filters	Your Prestige uses Protocol Filters to decide whether or not to allow passage of a data packet and/or to make a call. Protocol filters act on IP/IPX packets and can serve as a limited firewall.
Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy Servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server, via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
PSTN	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and callee.
PVC	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
ras	This is the name of the firmware on the Prestige. Renaming may be necessary when uploading new firmware to the Prestige.
RBOC	Regional Bell Operating Company. There are currently seven regional telephone companies that were created by the AT&T divestiture.
RFC	A Request for Comments is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the

	final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.
RIP	Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.
Rom-0	This is the name of the configuration file on the Prestige. Renaming may be necessary when uploading a new configuration file to the Prestige.
Router	A device that connects two networks together. Routers monitor, direct and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.
SAP	In NetWare, the Service Advertising Protocol broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.
SDSL	A Symmetrical Digital Subscriber Line is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire. It can provide data rates up to the T1 rate of 1.544 Mbits/sec, and it operates above the voice frequency, so voice and data can be carried on the same wire.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
SMT	System Management Terminal. The SMT is a menu-based interface that you use to configure your Prestige.
SNMP	System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
SOCKS	A protocol that handles TCP traffic through proxy servers.
Static Routing	Static routes tell the Prestige routing information that it cannot learn automatically through other means. The need for Static Routing can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.
STP	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.

Straight Through Ethernet Cable	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight through Ethernet cable is the most common cable used.
SUA	Single User Account. The Prestige's SUA feature allows multiple user Internet access for the cost of a single ISP account. See also NAT.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP Address that you entered. You do not need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.
Syslog	An abbreviated form of System Log. Using the UNIX syslog facility, the Prestige records (logs) phone calls or creates a CDR (Call Detail Record). Syslog is an administrative tool that assists accounting and is configurable via the SMT.
TCP	Transmission Control Protocol handles flow control, packet recovery, IP providing basic addressing and packet-forwarding services.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
Terminal Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
TFTP	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
Twisted Pair	Two insulated wires, usually copper, twisted together and often bound into a common sheath to form multi-pair cables. In ISDN, the cables are the basic path between a subscriber's terminal or telephone and the PBX or the central office.
UDP	User Datagram Protocol is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.
UNIX	A widely-used operating system in large networks.
URL	A Uniform Resource Locator is an object on the Internet or an intranet that resides on

	<p>a host system. Objects include directories and an assortment of file types, including text files, graphics, video and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.</p>
VC-based Multiplexing	<p>By prior mutual agreement, each protocol is assigned to a specific virtual circuit, eg., VCI carries IP, VC2 carries IPX, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.</p>
WAN	<p>Wide Area Networks link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems and satellite systems.</p>
WWW	<p>World Wide Web. Frequently used when referring to "The Internet", WWW has 2 major meanings. One, loosely used, the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Two, the universe of hypertext servers (HTTP servers).</p>
XDSL	<p>Digital Subscriber Line(s) where x, when specified, denotes a particular flavor of DSL, eg., ADSL, G.SHDSL, SDSL, VDSL, RDSL, etc.</p>

Index

- I*
- 10/100 MB Auto-negotiation 1-2
- A*
- Anonymous Login Type 10-16
- Application Scenario 1-4
- AT Command 10-9
- ATM Adaptation Layer 5 (AAL5) 3-10
- Authentication 4-3, 4-4
- auto-negotiation 1-2
- B*
- Backup Configuration 10-10
- Backup successful
- sample 10-10
- Binary Mode 10-17
- Booting Up 2-8
- Bridging 2-10
- Ether Address 7-4
- Ethernet 7-1
- Ethernet Addr Timeout 7-3
- Remote Node 7-2
- Static Route Setup 7-3
- C*
- Call Filtering 8-1
- Call Filters
- Built-In 8-1
- User-Defined 8-1
- Canadian Users, Information v
- CDR 10-6, 10-7
- CDR (Call Detail Record) 10-5
- CHAP 4-3
- CHAP (Challenge Handshake Authentication Protocol) 1-2
- Collision 10-3
- COM port 2-3
- Command Mode 10-19
- Community 9-2
- Compression 4-5
- Configuration
- default A
- Configuration
- Internet Access 3-9
- Configuration File 10-9
- Connect your Prestige 2-2
- Console Port 2-3
- Copyright ii
- cost of transmission 4-7, 5-4, 5-7
- Country Code 10-4
- CPU Load 10-3
- Customer Support ix
- D*
- Data Compression 1-2
- Data Filtering 8-1
- Device Filter rules 8-14
- DHCP 1-2, 3-1, 10-4
- DHCP Setup 3-5
- Diagnostic 10-8
- Diagnostic Tools 10-1
- Dial Backup 1-3
- Directory
- Local 10-16
- Remote 10-16

DNS	See Domain Name System
DNS proxy	3-2
Domain Name	E
Domain Name System	3-2
DOS Prompt	10-15
Download	10-9

E

Encapsulation	1-3, 3-10, 4-2, 4-5
ENET ENCAP	1-3, 3-11
ENET ENCAP Encapsulation	3-11
ENET ENCAP Gateway	3-14
Error Log	10-5
Error/Information Messages	
Sample	10-5
Ethernet	2-11
Ethernet parameters	3-1
Ethernet Traffic	8-18
Ethernet/802.3 bridged	1-4
Exit SMT	2-6

F

Factory Ethernet Defaults	3-1
FCC	iv
Features	1-1
Filename Conventions	10-9
Filter	8-1
Applying Filters	8-18
Ethernet Setup	2-12
Ethernet traffic	8-18
Ethernet Traffic	8-18
Example	8-15
Filter Rules	8-5
Filter Structure	8-3
Generic Filter Rule	8-10

Remote Node	4-8
Remote Node Filter	4-8
Remote Node Filters	8-18
Sample	8-16
Sample telnet filter	8-15
SUA	8-14
TCP/IP Filter Rule	8-6
Filter Log	10-6, 10-7
Filter Rule	8-7
Filter Rule Process	8-2
Filter Rule Setup	8-6
Filter Rules Summary	
Sample	8-17
Filter Set	
Class	8-6
Filter Set Configuration	8-3
filter type	8-5
Filtering	8-1, 8-6
Filtering Process	
Outgoing Packets	8-1
Filters	
IPX Filter Rule	8-12
firewall protection	3-15
Firmware Upgrade	1-3
firmware version	10-4
Flash ROM	10-11
Frame types	6-1
Front Panel	2-1
FTP Command	10-15
FTP Session	
sample	10-16

G

G.991.2 ITU	xxiii
G.SHDSL	xxiii, 1-1

G.SHDSL Benefits	xxiii
Gateway.....	3-2, 5-7
Gateway Node	6-7, 7-4
General Setup	2-9

H

Hardware Installation	2-1
hop count.....	4-7, 5-4, 5-7
Hop Count	6-6, 6-7
HTTP.....	F, J, M
HyperTerminal program.....	10-10
HyperTerminal Screen.....	10-10

I

IANA.....	3-3
IGMP (Internet Group Multicast Protocol)	3-4
IGMP support.....	3-6, 4-7, 5-5
Initial Screen	2-3
Initial Setup	2-1, 3-1
Installation	
Ease	1-3
Installation Requirements.....	2-1
Interactive Applications	11-1
Internet Access	1-1
Internet Access Application	1-4
Internet Account Information.....	3-12
Internet Assigned Numbers Authority.....	See IANA
IP address	3-1
IP Address.....	3-2, 3-3, 3-6, 3-14, 3-15, 4-4, 4-6, 5-3, 5-4, 5-7, 7-4, 8-8, 10-4, 10-8, 10-17, 10-19, 11-3
IP Address Assignment	3-11
IP Alias.....	3-7
IP Alias Setup.....	3-7
IP Filter	8-9
Logic Flow	8-9

IP mask.....	8-7
IP Multicast	1-1, 3-4
Internet Group Management Protocol (IGMP).....	1-1
IP Packet	8-10
IP Policies	11-5
IP Policy Routing	1-2
IP Policy Routing (IPPR)	1-2, 3-4
Applying an IP Policy	11-5
Ethernet IP Policies	11-5
Gateway.....	11-5
IP Pool.....	3-1, 3-6
IP Protocol	11-4
IP Routing Policy	11-4
IP Routing Policy (IPPR)	11-1
Benefits	11-1
Cost Savings.....	11-1
Criteria	11-1
Load Sharing	11-1
Setup	11-2
IP Routing Policy Setup	11-3
IP Static Route	5-5
IP Static Route Setup	5-6
IPCP (IP Control Protocol)	3-2
IPX	
Ethernet Setup.....	6-4
External Network Number	6-2
Frame Types.....	6-1, 6-4
802.2.....	6-1
802.3	6-1
Ethernet II.....	6-1
SNAP(Sub-Network Access Protocol).....	6-1
Internal Network Number.....	6-2
LAN-to-LAN.....	6-4
Prestige.....	6-3
Remote Node Setup.....	6-5
Seed Router	6-3

Static Route Setup.....	6-6
IPX Environment.....	6-3
IPX Network number.....	6-4
IPX Network Number.....	6-1
IPX Node Number.....	6-1
IPX Packet Type.....	8-13

L

LAN.....	10-2, 10-3
LAN IP.....	3-9
LAN with Server.....	6-3
LAN without Server.....	6-3
LAN-to-LAN Novell IPX.....	6-5
LED Functions.....	See
LED indicators.....	2-1
LEDs.....	See LED indicators
Link type.....	10-2
LLC-based Multiplexing.....	3-10, 5-2
Log and Trace.....	10-5
Log Facility.....	10-6
logging option.....	8-8, 8-11, 8-14
Login.....	4-3
login screen.....	2-4
Login Type.....	10-16

M

MAC.....	See Media Access Control
MAC address.....	7-4
Main Menu.....	2-6
Main Menu Commands.....	2-6
Management Information Base (MIB).....	9-2
Maximum Burst Size (MBS).....	3-14
MBS.....	See Maximum Burst Size
Media Access Control.....	6-1, 7-1
Message Logging.....	10-5

Metric.....	4-7, 5-4, 5-7
Multicast.....	3-6, 4-7, 5-5
Multicasting.....	3-4
Multiple Protocol over ATM.....	1-3
Multiple Protocol Support.....	1-2
Multiple Server Configuration.....	3-18
Multiplexing.....	3-10, 4-2
My WAN Address.....	4-7

N

NAT.....	8-15
Netmask.....	3-2
NetWare.....	6-1
NetWare Network Numbers.....	6-2
NetWare server.....	6-1
Network Address Translator (NAT).....	3-15
Network Management.....	1-3
network number.....	3-3
NIC (Network Interface Card).....	2-1
Novell IPX Ethernet Setup.....	6-4

P

Packet	
Error.....	10-2
ICMP Ping.....	10-3
Received.....	10-3
SAP Broadcast.....	10-3
Transmitted.....	10-2
Packet Triggered.....	10-6, 10-7
Packets.....	10-2
PAP.....	4-3
PAP (Password Authentication Protocol).....	1-2
Password.....	2-4, 2-7, 4-3, 9-2
Path	
Local.....	10-16

Configuration.....	3-16
Single User Account Topology.....	3-15
SMT Interface Navigation.....	2-4
SMT Main Menu.....	2-6
SNMP.....	1-1
Community.....	9-3
Configuration.....	9-2
Get.....	9-2
Manager.....	9-2
MIBs.....	9-2
Trap.....	9-2
Trusted Host.....	9-3
Socket.....	6-7
Source-Based Routing.....	11-1
speed	
default.....	A
Speed.....	1-1
Stac Compression.....	4-5
Stac Data Compression.....	1-2
Static Route Setup.....	5-5
Static Routing Topology.....	5-6
SUA.....	1-3
Multiple Servers.....	3-17
subnet mask.....	3-1
Subnet Mask.....	3-2, 3-3, 3-6, 4-7, 5-4, 5-7, 10-4
Successful Restoration	
Sample.....	10-12
Sustain Cell Rate (SCR).....	3-14
Syntax Conventions.....	xxi
Syslog.....	10-5
Syslog IP Address.....	10-6
syslog server.....	10-5
System	
Backup Configuration.....	10-9
Boot module commands.....	10-17
Command Interpreter Mode.....	10-18

Console Port Speed.....	10-4
Diagnostic.....	10-8
Firmware Update.....	10-12
Log and Trace.....	10-5
Restore Configuration.....	10-11
Syslog and Accounting.....	10-5
System Information.....	10-4
System Status.....	10-1
TFTP Transfer.....	10-14
Upload Router Firmware.....	10-12
Uploading Router Configuration File.....	10-13
System Maintenance.....	10-1, 10-19
System Management Terminal.....	2-4, K
System Name.....	2-9
System Status.....	10-2

T

TCP datagrams.....	3-16
TCP/IP.....	5-1, 8-14, 10-8, 10-9, F, G, H, K, L
TCP/IP Ethernet Setup and DHCP.....	3-1, 3-2
TCP/IP Options.....	5-1
TCP/IP Setup.....	3-6
TFTP transfer.....	10-15
third-party FTP client.....	10-16
third-party TFTP client.....	10-17
Tick Count.....	6-6, 6-7
Time and Date Setting.....	10-18, 10-19
Time Zone.....	10-19
TOS (Type of Service).....	11-1
Trace Records.....	10-5
Transfer Rate.....	10-3
Transfer Type.....	10-16
Type of Service.....	11-1, 11-3, 11-4, 11-5

U

UDP.....	3-16
Unicast.....	3-4
UNIX Syslog.....	10-5, 10-6
UNIX syslog parameters	10-6
Upload.....	10-9
Upload Firmware.....	10-12
Upload Router Configuration File.....	10-14
UTP	2-3

V

VC-based multiplexing.....	4-2
VC-based Multiplexing	3-10, 5-1
VCI (Virtual Channel Identifier).....	3-10
VPI (Virtual Path Identifier).....	3-10

W

Wall-Mounting.....	1-3
WAN address	5-4
WAN IP	3-9
WAN Setup.....	2-10, 2-11

X

xDSL, what is it?.....	xxiii
XMODEM Protocol.....	10-10
XMODEM upload.....	2-8

Z

ZyNOS	10-4, 10-9, 11-2
ZyNOS F/W Version.....	10-9
ZyXEL Limited Warranty.....	viii